ePDQ

User Guide

V5.0 Released March 2009

Software Version: 5.9 Payment Engine & Internet Authentication

Doc Version Control

Version No.	Date Issued.	Reason for Change
2.0	July 2005	Card Scheme rules changes for Switch, Solo and Maestro cards
		Important message about fraud policy
		Fraud Rule Weighting
		Address Normalisation
3.0	October 2006	Address Verification Service response correction
		MasterCard SecureCode Liability Shift Revisions
4.0	August 2007	Application upgrade to version 5.9
		Password policy
		Reporting
		Additional currencies
		Risk Management
5.0	March 2009	Re-brand
		Risk Management

Contents

Introduction

Welcome to the ePDQ User guide. This guide provides you with the essential information required to successfully use ePDQ and its features.

Upon successful application to ePDQ, you will be provided with a number of documents that provide complete and comprehensive detail on the many functions and operations supported by the ePDQ payment engine, ePDQ CPI, ePDQ MPI and ePDQ Store Admin. You must familiarise yourself with the documents specific to the product you have chosen to obtain a full and complete understanding of how to use ePDQ effectively.

The relevant documents are:

ePDQ CPI Merchants:

- CPI Integration Guide
- CPI Integration Enhancements
- Store Administrator Guide
- Risk Management Guide

ePDQ MPI Merchants:

- Store Administrator Guide
- Risk Management Guide
- API Guide/XML Guide where appropriate.
- Document Hierarchy
- Payment Reference (Barclays)

ePDQ Lite Merchants:

- Store Administrator Guide
- Risk Management Guide
- ePDQ Lite Quick Start Guide

Please contact our eCommerce Support Team, quoting your merchant or ePDQ store number if you are unsure which product you are using or if you do not have copies of any of these documents.

If you are using a Merchant Development Partner or Web Developer, the URL where documentation can be downloaded from may have been provided direct to your developer.

This document relates to version 5.9 of the ePDQ Payment Engine.

Contacting us

Contact us on 0844 822 2099*

Monday to Sunday:	8.00am to midnight

Alternatively you can email us at: epdq@barclaycard.co.uk

*** Calls may be monitored or recorded to maintain high levels of security and quality of service**

How to use this Document

This document combines essential user information, references to the main documents, plus tips on how to get the most from the ePDQ products. For ease of use, it is indexed by Section, Topic and Product as shown below:

Section	Topic	Products
C Reports	How to View Transactions	CPI MPI Lite

Main Document Reference	Store Administrator Guide. Chapter 5. Page 85

This type of header will appear at the start of each new subject. There are 5 **Sections** A, B C, D and E.

The **Topic** provides information on what can be performed by ePDQ within the section. You can "mix and match" the topics within the sections to tailor this user guide to your specific needs.

The **Products** listing details which products the section is relevant to.

Section	Content	Description
A	Basic Access	Include logging on, password allocation, access control and using the facilities offered by the ePDQ Administration Tool
B	Orders	How to process transactions (via Point of Sale)
C	Reports	How to use the many different reporting options available
D	Risk & Fraud	How to effectively use the rules, lists and other fraud tools to help identify potentially fraudulent transactions through your store
E	Administration	Information on the configuration of your store

The Main Document Reference section details where in the standard product documentation, further information can be found.

Top 10 ePDQ Tips

Before using ePDQ to process transactions, it is important that you understand some key principles of how the product operates. To get you started, we have provided a list of ten tips that you should consider. Where relevant, section references for further information in this guide are provided.

1. Before you can trade using ePDQ you must request activation of your account. To do this, complete the "account activation form" on the next steps web page as indicated on your welcome letter. Once you have activated your store, transactions must be processed in Production (P) mode. All other processing modes are test modes.

IMPORTANT! It is your responsibility to ensure that transactions are processed correctly. We are not in a position to advise you should you submit transactions in test mode inadvertently.

2. If you activate any of the strategy rules, you may decline a transaction that has been authorised by the card issuer. Have a clear fraud policy in place and prepare procedures for dealing with potentially fraudulent transactions.

3. We recommend you always use the **Current Batch** within **Orders** or **Settlement Reports** within **Reports** to assist you with reconciliation. These will confirm which transactions have been paid to you.   See section B.

4. If you have activated any strategy rules, regularly check the **Fraudulent** and **Review** reports within **Risk Management**. There may be transactions listed that require attention.   See section D.

5. **PreAuth** transactions will not be processed until they have been marked as shipped. Check the Unshipped report regularly to ensure that there are not any transactions waiting to be shipped. See section B. *PreAuth, is not permitted for Solo or Maestro cards

6. Ensure that any **PreAuth** transactions for goods/service that cannot be delivered (ever) are voided, as this will help with reconciliation. See Section B. *PreAuth, is not permitted for Solo or Maestro cards

7. If a **Partial Credit** is required, the sub total must be amended to the amount that you wish to refund before selecting **Partial Credit**. If not amended, it will generate a full refund. You need to specify the amount to be refunded and not the new value.

8. If you use a third party to integrate ePDQ on your behalf please ensure that you restrict the user permissions to ensure they do not have access to your store once live.

9. Only alter the **Settlement** settings if you have agreed the changes with us.

10. All store alterations must be requested through the support team.

Section	Topic	Products
A Basic Access	**How to Log On/Out**	CPI MPI Lite

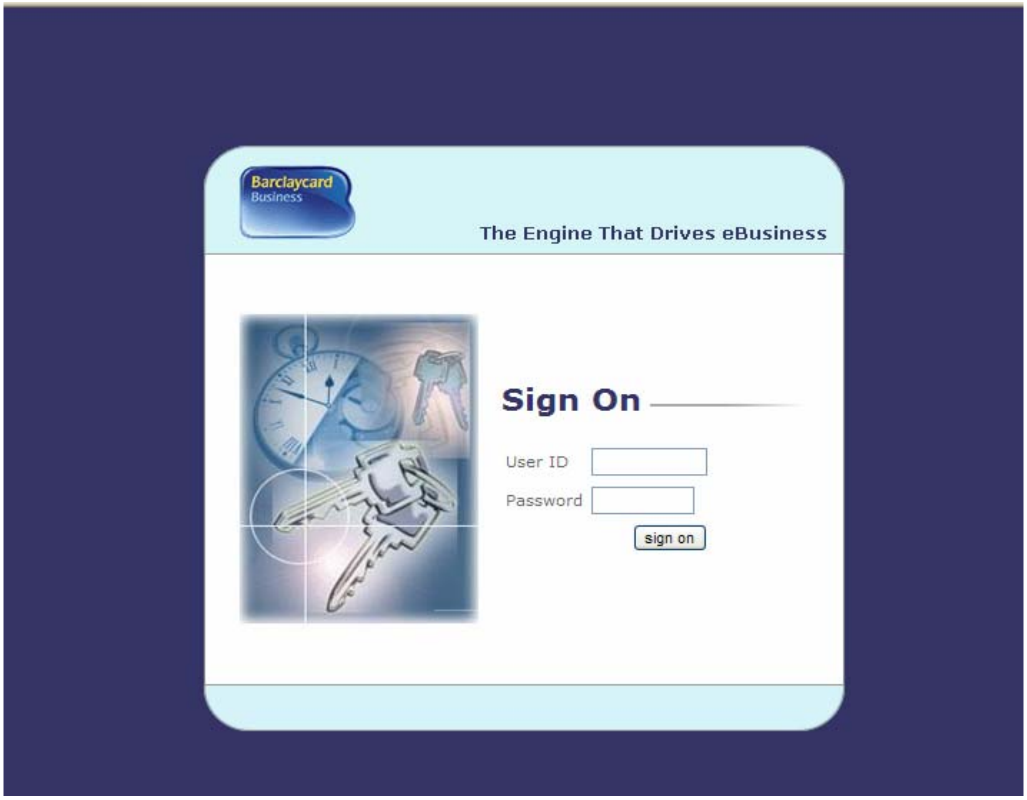
Main Document Reference	Store Administrator Guide. Chapter 5. Page 34

Logging On

The ePDQ product is supported by a very comprehensive Store Admin Tool. This allows you to view orders, perform transactions, set strategy rules and manage your ePDQ store.

You access your store via a secure URL. When we initially set up your ePDQ store, you, or your nominated web developer will receive an email confirming your store details. This will contain the unique store ID (a numeric value), the URL from which you can access your store, a user ID and a prompt for you to call us for your password.

Upon receipt of the mail you must contact the eCommerce Support Team on 0844 822 2099 to obtain your password. Once obtained, you should click the URL link sent in the email to access your store.



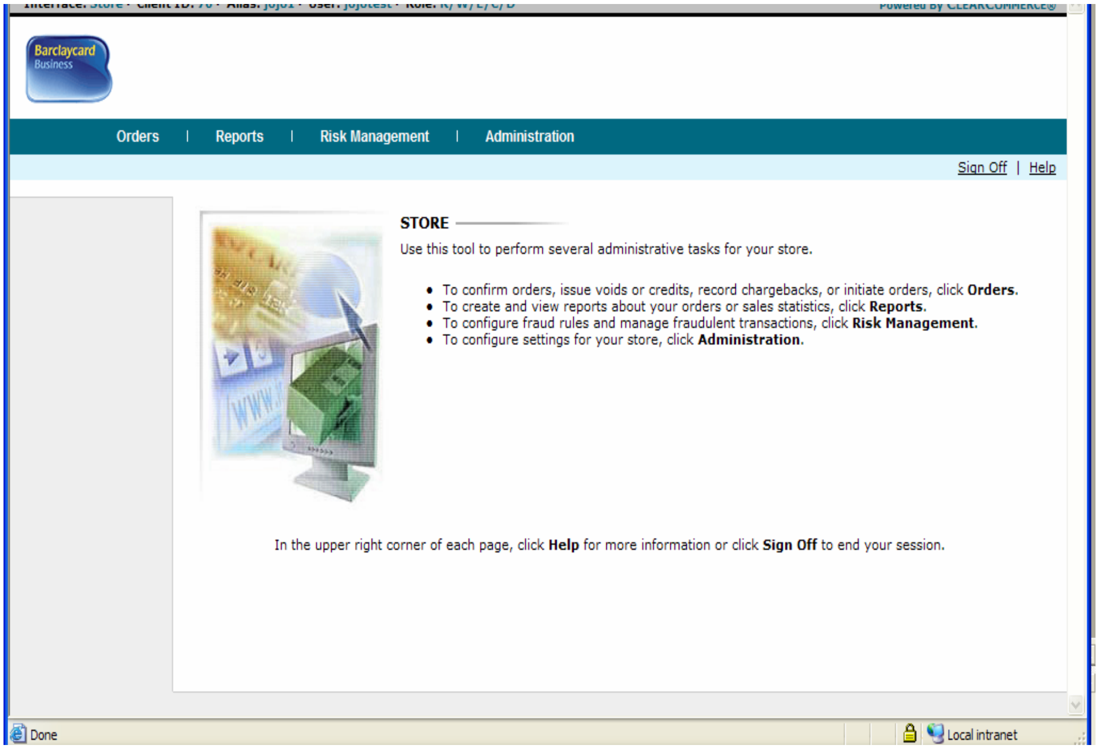
You must log into your ePDQ store using the log in details we provide to you. Upon successful login you are able to set up further users and can either change or delete the initial password provided to you. You will have three attempts to log into your store. If, after the third attempt, you fail to enter the correct details your store will be locked. You will need to contact us to unlock your store.

Once successfully logged into your store, you will see the set up information displayed as shown below:

This shows:

Interface – this will always be Store.

- **Client ID –** this is the unique ID for the store.
- **Alias** – this is an alternative alias that can be assigned to the store, i.e. "Mystore".
- **User –** this is the name of the user accessing the store.
- **Role –** this is the role with associated permissions that the user has within the store.



Interface: Store · Client ID: 70 · Alias: jojo1 · User: jojotest · Role: R/W/E/C/D

Powered By CLEARCOMMERCE®

STORE

Use this tool to perform several administrative tasks for your store.

- To confirm orders, issue voids or credits, record chargebacks, or initiate orders, click **Orders**.
- To create and view reports about your orders or sales statistics, click **Reports**.
- To configure fraud rules and manage fraudulent transactions, click **Risk Management**.
- To configure settings for your store, click **Administration**.

In the upper right corner of each page, click **Help** for more information or click **Sign Off** to end your session.

Using the Store Admin Tool

Once successfully logged in, you are able to navigate the store. There are four main options available, which are explored in more detail later in this user guide. The main areas are:

- **Orders** – this allows you to manage your orders on a day to day basis for the purposes of reconciliation, or to perform basic transactions.
- **Reports** – provides you with management information on all transactions processed and settled through your store.
- **Risk Management** – supports comprehensive risk management tools to help identify and minimise fraudulent transactions through your store.
- **Administration** – controls the store configuration.

Obtaining Help

You can use the on-line help tool supplied with your ePDQ store at any time by clicking on the "Help" link in the top right hand corner. This displays a full index of features available, and provides useful tips for how to operate your store.

We strongly recommend that you familiarise yourself with the help screens.

Error Message When Logging In

If the role assigned to your user does not have the correct permissions to log into your store, or you have incorrectly entered your details, you will see an error message that reads "Insufficient permissions to perform requested operation".

You should first check that your role allows to you log in (See the topic on Roles) and also check you have entered your user ID and password correctly. This message may also be seen if you attempt to do something in the store that your role prohibits.

Logging Out

Whenever you have completed activity within the store you must log out. This prevents unauthorised access to your store as the password and user ID will be required to log back in.

To log out, simply select "Sign Off" on the top right hand corner of your store.

If your store remains inactive for more than 30 minutes you will be logged out automatically. You will need to re-enter your user ID and password to gain access.

TIP! Do not just close your browser to sign out of the store. This will not sign you out correctly and could allow unauthorised access if someone re-opens your browser.

Section	Topic	Products
A Basic Access	**Controlling Access to your Store**	CPI MPI Lite

Main Document Reference	Store Administrator Guide. Managing Users. Page 48

Managing Users

When your ePDQ store is initially set up, we will provide you with a user ID that allows full permissions across your store. The set of permissions allocated to the user is defined by which Role we have allocated. Typically we will allocate an "ePDQ Level 4" role which gives you full permissions.

You can create new users with different role allocations, allowing different access levels throughout the store.

Store users only have access to the store they are allocated to. As long as you have the correct permissions, you can set up new store users. The process is described below:

1. After you have logged into the store, click **Administration** from the top four options.
2. Select Users from the menu on the left. The User Configuration Page displays all currently configured store users. To work with a user, you need to click the "select" button. From this page, you can:
   - **View** the selected users permissions
   - **Add** a new user and assign it a role
   - **Update** a selected users configuration
   - **Delete** a selected user
3. Depending on what option you select, you will be required to complete details as indicated on the screen. Details of how to add a user follow this section.

TIP! If you make any changes to an existing user to change the page display size or role assigned to them, that user will have to sign off and back in again before the changes are effective.

Section	Topic	Products
A Basic Access	**Roles, Permissions and Actions**	CPI MPI Lite

Main Document Reference	None

Each and every user that accesses either your ePDQ store, or submits transactions using the ePDQ CPI and MPI will be allocated certain user permissions. These are grouped together under the headings of "Roles". These are, in essence, profiles that determine what that user is able to do, and can also prohibit them for undertaking certain activities.

Roles can be broken down into:

- Role Configuration

  This is the high level setting for the role. Typically a role is used for a standard type of activity. For example, if the role is "ePDQ Level 1", then this would be associated to a user who performed simple operations within ePDQ.

- Resources

  Describes the type of functions you want the role to do. For example, one of the resources of ePDQ level 1 will be "Payment Transactions" which would allow them to perform defined transactional activities.

- Actions

  Within each resource, you can allocate specific actions. There are a range of actions that are allocated to you. As administrators we will also have specific actions allowing us to perform high level tasks. The actions most commonly assigned to store level roles are:

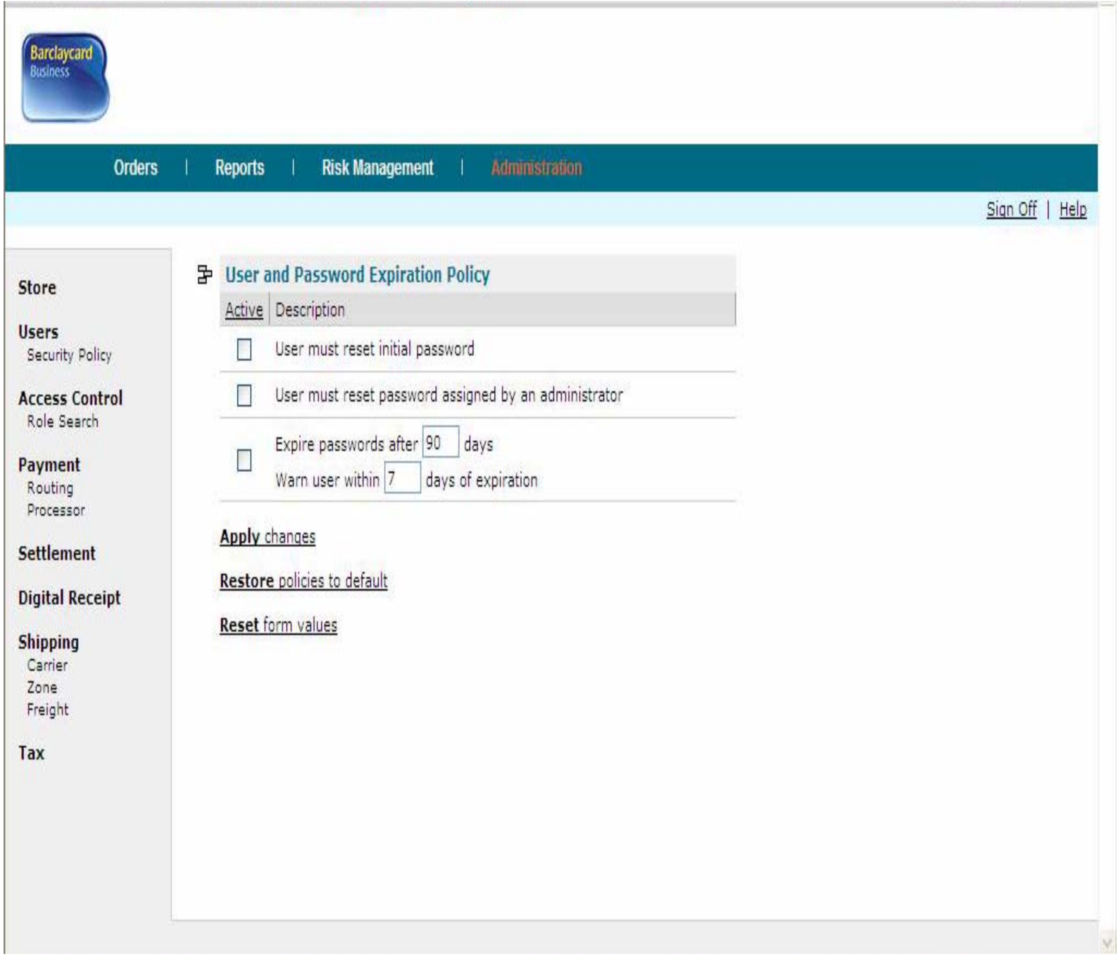
  - **Get –** this allows you to retrieve/read data.
  - **Add –** this allows you to add new items such as a new user, or fraud rule
  - **Update –** Allows you to update information such as store details.
  - **Delete –** Allows you to delete information such as user details.
  - **Execute –** this is required to perform activities such as submit transactions.

The Roles available to you can be found in the Role drop down list. There are a number of roles available. ePDQ has four specific roles created which we recommend you adopt. These are detailed in the next section.

Section	Topic	Products
A Basic Access	Password Security Policy	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 4 Page 49

Changing passwords on a regular basis can help tighten security, and the best way to ensure that passwords are changed regularly is to have them expire regularly. When a user's password expires, that user cannot sign-on to the ePDQ Administration Tool until he or she changes the password.



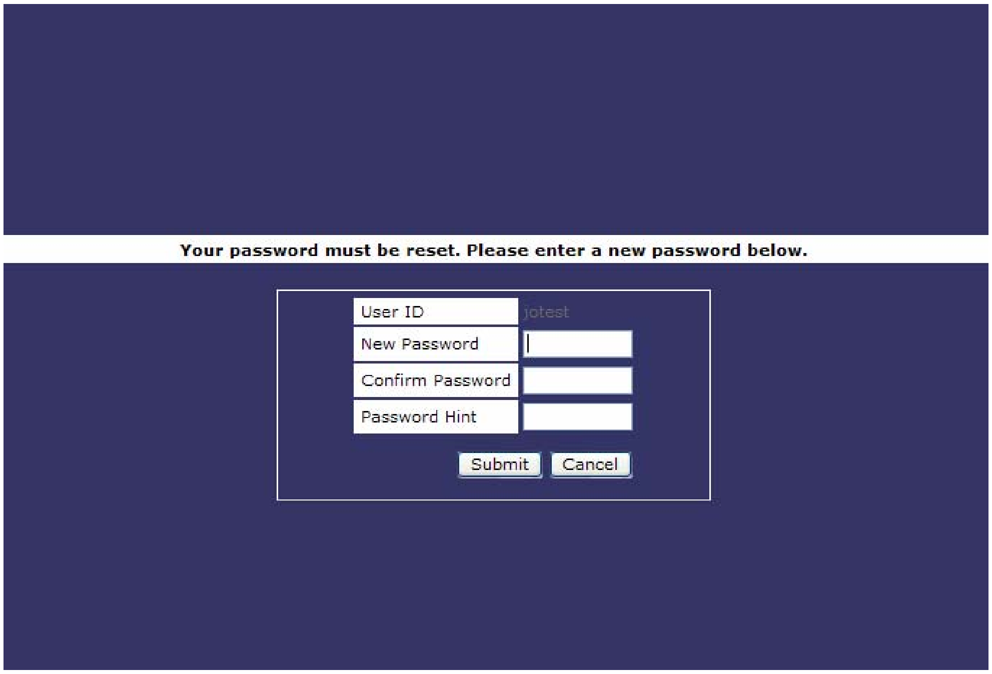
User and Password Expiration Policy

Active	Description
□	User must reset initial password
□	User must reset password assigned by an administrator
□	Expire passwords after 90 days Warn user within 7 days of expiration

To manage password expiration, you can define the following:

The amount of time that a password can be used on the ePDQ Administration Tool for example, if the password expiration is set to a 30-day time interval, a user cannot use a password for more than 29 days. You can also set the ePDQ Administration Tool to warn the user within a configurable time that the password is going to expire.

A user’s password also can be configured to expire at the first login or after the password is reset by an administrator. The initial password issued by an administrator is valid for the user's first login only. At that time, ePDQ prompts the user to choose another password before any other work can be done. This way only the person assigned the userid knows the password.



Your password must be reset. Please enter a new password below.

User ID jotest

New Password

Confirm Password

Password Hint

IMPORTANT - If you have elected to use the ePDQ Cardholder Payment Interface (CPI) to submit transactions to the ePDQ engine, you must allocate a user to perform the basic transaction requests.

If you have enabled the password security policy within your ePDQ store you must ensure that the specific CPI user and password never expires. Always select the ‘Password never expires’ option to avoid this user and password expiring.

This user will be required for the “behind the scenes” transaction processing performed by the CPI and must be maintained at all times (it must not be deleted or modified).

Section	Topic	Products
A Basic Access	**Set Up and Amend Password Security Policy**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 4 Page 51

To set the User Security Policy

1. After you have logged into the store, click **Administration** from the top four options.
2. Select **Security Policy** from the menu on the left. The **User and Password Expiration Policy** screen is displayed.
3. Select the Policy options that are appropriate for your own security policy then select **Apply these changes.**
4. The Policy will now apply to all Users within your ePDQ store

Once the security policy has been applied you may want to amend the policy of a specific user e.g. You may have allocated a user specific for transaction processing with the ePDQ Cardholder Payment Interface and this user profile should never expire.

To amend the security policy for a specific user

1. After you have logged into the store, click **Administration** from the top four options.
2. Select **Users** from the menu on the left. The **User List** is displayed.
3. Select the User profile and then select update. The **Update User screen** is displayed.
4. Apply the relevant changes e.g. select Password never expires then select update.
5. The changes will be applied and you will return to the **User list**.

Important – If you are creating a new password we recommend that you do not use the option to '**Allow the system to create the password'**

Section	Topic	Products
A Basic Access	**Default Roles**	CPI MPI Lite

Main Document Reference	None

As the roles based permission functionality of ePDQ is complex, we have set up four standard roles for your use in the store admin. When we first set up your store, we will allocate you a user that has been allocated the "ePDQ Level 4" role.

The details of the recommend store admin roles are provided below.

ePDQ Level 1

- Log in to your ePDQ store.
- Submit sales transactions only. Refund and Void are not permitted.
- View Orders & Periodic Billing Reports only. This will be read only access.

ePDQ Level 2

- Log in to your ePDQ store.
- Submit all transaction types (including refunds and voids).
- View Orders, Periodic Billing, Current Batch, Settlement and Transaction reports. These will be read only.

ePDQ Level 3

- Log in to your ePDQ store
- Amend digital receipt configuration
- View Fraudshield, Orders, Periodic Billing, Current Batch, Settlement
- Items, Roles and Transaction reports

ePDQ Level 4

This role is capable of all permissions associated with previous roles and has overall administrative access to your store. This is the default role provided with your initial user.

- Log into your ePDQ store
- Amend digital receipt configuration
- Allocate roles to users and unlock users
- Security policy password management
- View all reports
- Activate, deactivate and add new strategy rules
- Perform all transaction types

Section	Topic	Products
A Basic Access	**Adding a New User**	CPI MPI Lite

Main Document Reference	Store Administrator Guide. Managing Users. Page 48

When you add a new user to your store, the most important consideration is which role profile you wish to assign to the user. You may wish to consider restricting access to your store for particular members of staff. This is useful to ensure that no confidential or company sensitive data is accessed by an unauthorised user.

The role profiles and permissions are detailed earlier in this Section. Follow the procedure below to add a new user to your ePDQ store.

1. From the **User Configuration** Page (as shown in "Controlling Access to your Store), select **Add**.
2. The **Add User** page will be displayed. Enter the details as required. Mandatory fields are marked with *.
    - The User ID must be at least 8 alpha/numeric characters and can be up to 32 characters. It must not contain any special characters (such as *,/,_,-).
    - The Password must be at least 8 alpha/numeric characters and must not contain any special characters (such as *,/,_,-).
    - Enter the Password again for validation purposes.
    - Enter a Password Prompt. This must not be your password and must not compromise the password (i.e. "same as user ID").
    - Password never expires is optional if the password security policy is enabled within your ePDQ store. Always select this if the password is going to be used for the integration of ePDQ
    - Account Name and Account Description are optional, and can be used to identify a user, or store (i.e. Northampton Store).
    - The Role is the level of permissions you wish to assign to the user. Use the drop down list to select an appropriate role.
    - Set Pagination size according to how much data you wish to have displayed on each page.
3. You can elect for an email to be sent to the user (or an alternative recipient) confirming set up of the new user.
4. Once you have entered all the details correctly, select **Add**. If you have entered any details incorrectly and wish to clear all fields, select **Reset**.
5. The new user will now be created, and can be viewed from the **User Configuration Page**.

IMPORTANT! Please remember that the functionality described in this document may not be available to all users. The role assigned to them may prohibit access to certain functionality. Please ensure you and your staff are familiar with your role privileges.

Section	Topic	Products
A Basic Access	**Setting Users for the CPI**	CPI

Main Document Reference	None

If you have elected to use the ePDQ CPI to submit transactions to the ePDQ engine, you must allocate a user to perform the basic transaction requests. This user will be required for the "behind the scenes" transaction processing performed by the CPI and must be maintained at all times (it must not be deleted or modified).

We have created a specific role that can be allocated to the CPI user.

You may task your web developer to integrate ePDQ on your behalf. If this is the case, you can arrange for the web developers user ID to be allocated the specific CPI role. This will enable the web developer to incorporate the user into the CPI configuration to perform transaction tasks but will not allow that developer wider access to your ePDQ store, once live.

To set up a specific CPI user you should create a new user following the procedure described on the previous page and allocate the role of "CPI Access".

The CPI Access Role allows:

- Connection to the ePDQ engine.
- Transaction processing for Auth, PreAuth and Periodic Billing.
- Configuration of strategy rules.

You are now able to assign this user ID to the ePDQ CPI. Full instructions on how to do this are provided in the ePDQ CPI Mandatory Requirements document.

IMPORTANT - If you have enabled the password security policy within your ePDQ store you must ensure that the specific CPI user and password never expires. Always select the 'Password never expires' option to avoid this user and password expiring.

Section	Topic	Products
B Orders	**Viewing Orders**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 77

Brief Description

The orders menu provides you with direct access to existing orders within your store. You can perform actions on any orders displayed including refund and void. You may wish to restrict access to the orders screens.

If you wish to create a new transaction, update an existing transaction or understand which transactions are to be settled you should use the orders option.

Viewing Orders

You have three main options within Orders. These are:

- **Orders –** this provides you with an Order Search Criteria screen. Under the main Orders menu you have two set reports:
  - **This Month** shows all approved orders within the current calendar month.
  - **Unshipped** displays all orders that have not been marked as shipped within the current calendar month. These orders will not be settled (paid to your bank account).
- **Current Batch**. This will show all transactions that will be settled the next time your ePDQ store is due to settle transactions. This may include refunds.
- **Point of Sale**. Enables you to manually enter transactions. This is predominantly used by ePDQ Lite merchants.

To view orders using the Order Search Criteria screen, follow the procedure below:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Orders** from the menu on the left. The **Order Search Criteria** screen is displayed.
3. Select the required search criteria. You can search by specific values (i.e. order ID), and/or by time (i.e. Last 21 days).
4. Select which **Optional Fields** you wish to see in the orders report.
5. Select **Search**. All orders meeting your search criteria will be displayed.

TIP! If your search returns no results, check the Transaction State and Transaction Result field. It may be that your transactions may all be approved, and you have searched for declined. If you specify a time period, ensure you have selected the radio button next to the search criteria.

Section	Topic	Products
B Orders	**Finding an Order by Order ID**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 78-79

The most common unique reference to identify a transaction will be the Order ID. This is either generated from your shopping basket software, or by the ePDQ payment engine itself. Cardholders will be able to quote their order ID to you in the event of a query.

To find an order by Order ID:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Orders** from the menu on the left. The **Order Search Criteria** screen is displayed.
3. Under the **Search by** drop down menu, select **Order ID**.
4. A new box appears that allows you to enter the order ID. Enter the order ID exactly as supplied to the cardholder. Note, the search is case and space sensitive and you are unable to specify a **Time** period.
5. Your search results will be displayed.

There are a number of other search options you can use to identify a transaction:

- **Time**. Allows you to specify a time period in which to search.
- **Account Number & Time**. This allows you to search by card account number, and time period. For example you may wish to identify how many times card number 4929123123123 was approved in the last 20 days. You can search using the full card number or first four and last four digits (i.e. 49293123).
- **Card Type & Time**. Rather than specify a card number you can search by card type. For example, how many Visa card transactions were fraudulent during the last two months.
- **Customer ID & Time**. Can be used if you allocate a specific customer ID to each cardholder shopping at your site. This cannot be used by ePDQ CPI merchants.
- **Group ID & Time.** This is of particular use if you submit periodic billing orders, or wish to group a segment of orders. The Group ID can be used to connect a series of orders.
- **Item ID & Time**. Of particular use if you are submitting orders made up of items (i.e. one order consisted of 12 separate parts). ePDQ MPI only.

Each time you use the search criteria you must ensure that you have correctly specified each search field before submitting, as your search criteria will not be remembered if you select back.

Section	Topic	Products
B Orders	**Finding Information on an Order**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 77-79

Each order submitted through the engine contains a historic record of how it was submitted, when and the results associated with it.

By following the procedure in "Finding an Order by Order ID" you will be presented with the **Order Detail** page. This displays information relating to the order, including tax, shipping and total amount, the transaction ID and any captured billing information.

The **Transaction Detail** section will contain all transactions relating to a particular order. For example, the initial authorisation would have one transaction ID, a subsequent refund would have a further transaction ID and the eventual settled amount could have a further ID. Each transaction ID will feature the status, time & date stamp and the amount.

By clicking on the **Transaction ID** you will open the **Transaction Detail** page and be able to see very detailed information relating to the order. This contains the complete history and status of the transaction. Please remember that the Transaction Detail page relates to each individual transaction within an order. The information contained for a sale transaction will be different to that held for a refund transaction.

The **Transaction Detail** page typically displays:

- **Status**. Confirms the current status of the transaction (i.e. Approved, Captured, Settled).
- **Payment Details**. Provides confirmation of the card details used. The card number will only display the first and last four digits.
- **Amounts**. Any amounts submitted including tax, shipping, discounts and total.
- **Order Details**. Typically the order ID.
- **Settlement Details**. This confirms which settlement batch the transaction was settled in. This can be used for reconciliation purposes.
- **Transaction Details**. Contains the transaction time & date stamp plus how the transaction was submitted (i.e. via the Point of Sale).
- **Processor Details**. Contains all responses associated with the transaction such as CV2, AVS, authentication and authorisation code.

Further examples of how to use the information within the **Transaction Detail** page are provided in Section D Risk Management as this allows you to confirm fraud rule responses.

Section	Topic	Products
B Orders	**Viewing Transactions Ready for Settlement**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 85

Every successful order processed through your store is put into a settlement batch, ready to be paid into your bank account.

Typically, ePDQ collects transactions from each store at the end of the day and sends them to the main Barclaycard Business acquiring system to be processed. This process is called settlement.

You can view which transactions are due to be settled by viewing the **Current Batch**. Any transactions listed here will be picked up at the end of the day, or whenever you have set your store to next settle transactions. (More information on how you control the settlement of your store can be found in Section D Administration).

To view the **Current Batch**:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Current Batch** from the menu on the left.
3. All orders that can be settled will be displayed. Next to each order will be an option of **Void**. This can be selected if you wish to cancel an order and not settle it.

To **Void** a transaction in the Current Batch:

1. From the list of orders displayed, select the ones you wish to Void by clicking the **Void** box on the order.
2. Once selected, click **Void** from the **Operations** menu on the left.
3. A **Transaction Management** screen will be displayed confirming that you have voided the transaction. If you have activated digital receipts, the cardholder will receive an email to advise that the transaction has been cancelled.

Any voided transactions will be removed from the current batch and will not be settled. Once a transaction has been voided you cannot alter its status (i.e. resubmit it).

You are able to view details on the order within the Current Batch by selecting either the Order ID or Transaction ID. This will display the order detail and transaction detail pages respectively. See "Finding Information on an Order" for details of what can be reviewed.

Section	Topic	Products
B Orders	**Manually Entering Transactions**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 101

TIP! This section is of particular relevance to merchants submitting transactions using ePDQ Lite.

You are able to enter credit or debit card details directly into the ePDQ payment engine by using the **Point of Sale** option. This captures all the relevant payment information and requests authorisation in the same way as a transaction submitted through a web page.

You can perform a number of different transactions through the Point of Sale, and can capture additional information (such as address) to be submitted. The following transaction types are supported through the Point of Sale:

- **Auth** (Default). Authorises the transaction and places it into the current batch ready for settlement. The cardholder will be charged for the transaction when the transaction is settled.
- ***PreAuth**. Authorises the transaction but does not place it in the current batch. This transaction requires manual intervention to place into the current batch. These types of orders are listed as **Unshipped** and must be marked as shipped before it can be settled.
- **PostAuth**. This can be used to change a PreAuth into a full Auth and place the transaction ready for settlement. If you select PostAuth you will be required to enter the original transaction ID of the PreAuth.
- **Credit**. Also known as "Refund". This can be applied to settled transactions only, and is used to pay back the value of the transaction to the cardholder.
- **Void**. This can be used to cancel and order that has not yet settled.
- **RePreAuth**. This can be applied to an existing PreAuth transaction that may have passed its original authorisation date (i.e. if you have a delay in stock availability). It will contact the card issuer and re authorise the transaction to ensure that funds are still available. As with a PreAuth transaction, you will need to mark the transaction as shipped before it is settled.
- **ReAuth**. Similar to above except for Auth transactions that have not yet been settled but may be in the current batch. Once the ReAuth is performed the transaction will be updated in the current batch.
- ***ForceInsertPreAuth**. Allows you to enter a new PreAuth transaction where you have obtained an authorisation code through voice authorisation.
- **ForceInsertAuth**. Allows you to enter a new Auth transaction where you have obtained an authorisation code through voice authorisation.
- **ForceUpdatePreAuth**. Allows you to enter a new authorisation code obtained via voice authorisations for an existing transaction. You will need to locate the existing transaction ID.

- **ForceUpdateAuth.** Allows you to enter a new authorisation code obtained via voice authorisations for an existing transaction. You will need to locate the existing transaction ID.

Note: Your customer will only be charged once for any forced transactions, as you obtain an authorisation manually. The ePDQ engine will not obtain an authorisation.

*** PreAuth, is not permitted for Solo or Maestro cards**

Section	Topic	Products
B Orders	**Performing a Manual Transaction**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 102

The default transaction type on the Point of Sale is Auth. This will authorise the transaction, and place it ready for settlement.

To perform an **Auth** from the **Point of Sale**:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Ensure that the Transaction Type is **Auth**.

For a basic transaction, you are only required to enter the mandatory details indicated by an *.

5. Enter the full **Card Number** with no spaces.
6. Select the **Expiry Date** from the drop down lists.
7. Enter the **Total** amount of the order. This must include any tax, shipping and discount.
8. You MUST select the **POS Environment** to match the type of transaction you are processing (either eCommerce for ePDQ CPI/MPI/Lite or Mail Order, Telephone Order for ePDQ Lite only). You are not permitted to use the eCommerce environment for International Maestro cards
9. Ensure the **Processing Mode** is set to **Production**.
10. Select **Process Transaction**. ePDQ will then obtain an authorisation code and deliver a **Point of Sale –** Receipt confirming the result of the transaction. If approved the transaction will be placed in the current batch, ready for settlement.

There are a number of optional fields available for a Point of Sale Auth transaction. If you decide to enter details they will require:

- **Group ID**. Used to link a number of order ID's together. You could use this to link a single customer to multiple orders. The Group ID must not exceed 36 characters and must not contain special characters (_, !?@V etc.)
- **Order ID**. A unique reference to identify the order. If you do not enter a value here, ePDQ will generate one for you. This can be provided to the cardholder and will be used to identify the transaction. The Order ID must not exceed 36 characters and must not contain special characters (_, !?@V etc.)
- **Card Verification Number**. This can also be known as CSC, CV2, Cvv2 and CVM and is the three digit security data on the back of most cards, or 4 digit data on the front of American Express cards. It is not the PIN number

- **Maestro/Solo Start Date.** This must be entered if the card you are processing is a Maestro /Solo card and has a start date specified. Select from the drop down list.
- **Maestro/Solo Issue Number**. Again, this must be entered if specified on the Maestro /Solo card you are processing. Enter the value exactly as specified on the card.
- **Shipping Amount**. This can be used to record the shipping amount but will not be used to calculate the total.
- **Tax Amount**. As above, this can be recorded for information processes, but will not be used to calculate the total.
- **Comments**. You can record any comment here relating to the order, which will be included in the **Order Detail**.
- **Charge Description**. This can be used to record any further information about the order and will appear in the **Transaction Detail** page.
- **Email Address**. Enter the email address of the cardholder if you wish to send them a digital receipt.
- **Processing Mode**. For live (real) transactions, this must be set to Production. There are a number of other options available:
  - **Approved**. This simulates an approved authorisation response and should be used for testing only.
  - **Declined**. This simulates a declined authorisation response and should be used for testing only.
  - **Random**. This simulates either an approved or declined response and should be used for testing only.
  - **Test**. This option should not be used.
  - **Risk Management** – Approved. This option should not be used.
  - **Risk Management** – Declined. This option should not be used.
- Full **Billing Information** details can be captured. Please enter details as indicated.

TIP! If you are planning to use the ePDQ Strategy rules for Address Verification, you must enter the full address details.

The **Periodic Billing Information** details are explained later in this section.

Section	Topic	Products
B Orders	**Performing Transactions such as Refund & Void**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Pages 89-95

This topic covers the procedures for performing the following transaction types:

- Refund (Credit)
- Partial Refund (Partial Credit)
- Void
- Pre-Auth
- Post-Auth

Refund

There are two types of refund available within the engine. You can either refund an existing order, or you can create an "independent" refund. This may be used when you are offering a customer a good will payment to their card, or if you cannot locate the original order details. You should restrict permissions to perform independent refunds.

To process a refund on an existing order:

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity.** If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to refund, select the Credit box on the order and then **Credit Orders** from the **Operations** menu on the left.
4. A **Transaction Management** page will be displayed confirming the refund. The credit on the transaction will be placed in the current batch and will be processed on your stores next settlement.

To process an independent refund:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction.**
4. Ensure that the Transaction Type is **Credit**. The required fields to enter the transaction will appear. Enter as much detail as possible. Ensure the **Processing Mode** is Production and then press **Process Transaction.**

Partial Refund

A partial refund can be used if you wish to refund only some of the order processed. This can be used if only part of an order has been returned, or where you are required to refund some monies following a specific customer request.

Again, you can either perform a partial refund on an existing order, or you can issue an independent credit for a partial amount. To do this, follow the procedure for processing an Independent refund.

To perform a partial refund on an existing order:

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity.** If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to refund click the **Order ID**. This will open up the **Order Detail** page. Within the Order Detail, will be a list of totals and a sub total.
4. Enter the amount you wish to refund in the **Subtotal field**. For example, if the order is for £1.00, and you wish to refund 28p, you should enter 0.28. This will then apply a partial credit of 28p, leaving a new total of 72p.
5. Once you have entered the refund amount, select **Partial credit** from the **Operations** menu on the left.
6. A **Transaction Management** page will be displayed confirming the refund.

You can view the refund applied by looking at the **Transaction Detail Page**. This will confirm the amount and date/time of any refunds applied.

Void

If you wish to cancel an order before it is settled, you can use void. This means that the transaction will not be passed for settlement and will not appear on the cardholder's statement. This is different to a refund in which both the original charge and subsequent refund will appear on their statement. You can only a void a transaction that has not yet been settled.

You can void a transaction either by locating it by using the Order search option, or by voiding it from within the current batch. This is probably the simplest approach:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Current Batch** from the menu on the left.
3. Identify the transaction you wish to void and select the Void check box.
4. Select **Void** from the Operations menu on the left.
5. A **Transaction Management** page is displayed confirming the action.

Pre-Auth

This type of transaction is useful if you are unable to fulfill an order immediately. You may wish to authorise the card to ensure that funds are available, but not charge the cardholder (i.e. settle the transaction) until you have the goods ready for distribution.

The procedure for processing a Pre-Auth transaction is similar to the process for Auth transactions. You must however ensure that you change the **Transaction Type** to **PreAuth.**

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Ensure that the Transaction Type is **PreAuth**.

Follow the remaining procedure for an Auth transaction. Remember that a PreAuth will not be settled until you take further action, by either marking the transaction shipped, or by processing a PostAuth on the transaction.

PreAuth is not permitted on Solo or Maestro transactions.

PostAuth

A PostAuth is the second half of a Pre-Auth transaction and updates it to be passed for settlement. If you wish to settle a Pre-Auth transaction you should follow the procedure below:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Select the Transaction Type of **PostAuth.** The required fields are displayed.
5. Enter the original PreAuth **Order ID.** This will be case and space sensitive.
6. Enter any other details available (optional).
7. Ensure the **Processing Mode** is **Production**.
8. Press **Process Transaction.**
9. A **Transaction Management** page will be displayed confirming the action.

Section	Topic	Products
B Orders	**Marking a Transaction as Shipped**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 86-89

Full Shipment

If you are submitting orders using the transaction type of PreAuth you need to "ship" the order before it is settled to your bank account. This process is referred to as shipping the transaction as it often relates to the time when you are physically ready to deliver the goods to the cardholder.

If you have taken a PreAuth order and are ready to send the goods and charge the cardholder you need to mark the transaction as shipped. The easiest way to do this is to use the Orders standard search of **Unshipped**. This will display all current orders that require action to ship them and pass them into the current batch.

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Unshipped** from the menu on the left. A list of all unshipped orders will be displayed. Each unshipped order will have a **Ship** box next to it.
3. Select the orders you wish to ship by selecting the **Ship** box and then select **Ship Orders** from the Operations menu on the left.
4. A **Transaction Management** page will be displayed confirming your action.

Partial Shipment

There may be occasions where you are unable to fulfill part of any order, and therefore wish to only charge the cardholder a partial amount.

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Ensure that the Transaction Type is **PostAuth**. The required fields will be displayed.
5. Enter the **Order ID** of the original PreAuth transaction.
6. Enter the amount you wish to ship in the **Total** field and press **Process Transaction**.
7. A **Transaction Management** page will be displayed confirming your action.

The remaining value of the transaction will expire and cannot be shipped.

TIP! If you regularly construct orders made up of many items, you should consider using the ePDQ MPI and use "items" when submitting orders. Further information can be found in the main API guide (ePDQ CPI & ePDQ Lite merchants cannot submit items).

Partial PostAuth

Sometimes, only some items in an order can be shipped immediately. In these cases, you might want to ship the available items and collect payment for these, deferring shipment of the remaining items and collection of payment for the remainder until later.

By default your store Partial Ship Follow-up settings will have been set to 'No follow-up transaction' in the 'Administration', 'Store' section. This means that once you have conducted the PostAuth for the items that have been shipped, the leftover part of the PreAuth will expire.

In order to process the deferred amount it is necessary for us to amend these settings, to 'Follow-up transaction, no PreAuth'. Please confirm the Store ID you require updating and we will configure your account accordingly.

Once this has been completed you can begin processing Pre Auth transactions in the knowledge that you will be able to settle the transaction in steps.

To partially ship an existing Pre Auth order, please follow the Partial Shipment instructions below (which can be found on page 32 of the ePDQ User Guide).

There may be occasions where you are unable to fulfill part of any order, and therefore wish to only charge the cardholder a partial amount.

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Ensure that the Transaction Type is **PostAuth**. The required fields will be displayed.
5. Enter the **Order ID** of the original PreAuth transaction.
6. Enter the amount you wish to ship in the **Total** field and press **Process Transaction**.
7. A **Transaction Management** page will be displayed confirming your action.

Once this process has completed a new, separate, transaction is automatically created for the remaining amount. This transaction has the same Order ID, but a different Transaction ID, to the original pre Auth request.

You may Post Auth against the Order ID as often as necessary until the full, original amount has been settled, or the order has been completed to the customer's satisfaction.

In the event that more than 7 days have elapsed since the original transaction date, you will need to obtain further authorisation using this new Transaction ID. To complete this you must initiate a RePreAuth to resubmit the transaction for approval.

Submitting a RePreAuth

1. After you have logged into the store, click Orders from the top four options.
2. Select Point of Sale from the menu on the left.
3. Check that the activity is Card Transaction.
4. Ensure that the Transaction Type is RePreAuth. The required fields will be displayed.
5. Click on Process Transaction and a new authorisation will be obtained.
6. Follow up with PostAuth as per previous instructions.

Section	Topic	Products
B Orders	**Handling Orders that "Refer" (Referrals)**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Appendix B Page 169 & 179

A referred transaction occurs when the cardholder's card issuer cannot approve the transaction straight away. Card Issuers may refer a transaction for any of the following reasons:

- The transaction amount is very high or the expenditure may be considered as 'out of character' for the cardholder.
- The transaction amount may be over the cardholders 'available to spend limit'.

Predominantly, in a card not present environment, issuers do not refer transactions (they will typically decline them) but some issuers may decide to use this option.

If a transaction is referred, you will need to contact our Voice Authorisations centre who in turn will contact the card issuer and obtain a voice authorisation code if the transaction can be approved. In some circumstances, the card issuer may decline the transaction.

Once you have obtained the voice authorisation code, you are able to process the transaction by using the ForceInsertAuth transaction type via the Point of Sale.

You will be advised that the transaction has been referred via a specific transaction response. Depending on which product you use to process transactions these will be:

- ePDQ CPI – "Awaiting Confirmation. Please contact the merchant and quote ref 2/3".

- ePDQ MPI – "Referral" (Error Code 2) or "Referral – Call bank for manual approval" (Error Code 3).

- ePDQ-Lite - Referral" (Error Code 2) or "Referral – Call bank for manual approval" (Error Code 3).

Should you receive a referred transaction, you need to take action to process the transaction. You may however take a business decision to not process the transaction, and could set up a fraud rule that rejects transactions based on the response codes above. See Table B12 on page 169 of the Store Administrator Guide for the response codes.

Section	Topic	Products
B Orders	**Finding Referred Transactions**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Appendix B Page 169 & 179

How to identify a Referred Transaction

Based on the error messages returned (as detailed on the previous page) you will know when a transaction has been referred. Because these transactions require manual intervention you will need to locate the transaction in your Store Admin. To locate the transaction within the Store Admin follow the procedure below:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Orders** from the menu on the left.
3. Search by **Order ID**, and enter the Order ID of the transaction.
4. Select Declined within the Transaction Result search criteria options.
5. Click **Search.**
6. The Order Detail page will display details of the order. Click on the **Transaction ID** within the Transaction Detail section to view information about the order.
7. The Transaction Detail page will show the 'Clear Commerce' response. If this is '2' or '3' this confirms the transaction has been referred.

TIP! If you wish to process the transaction, you will need to record the Transaction ID (not the Order ID). A simple option is to 'copy' the information so that you may 'paste' it later, if required.

Section	Topic	Products
B Orders	**Processing a Referred Transaction**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Appendix B Page 169 & 179

In order to process a referred transaction, you first need to follow the process on the previous page to identify the transaction. Once you have located the transaction, you should follow the procedure below to process. You may only process a referred transaction if you have access to the full card number.

1. Contact the customer to advise that the transaction has been referred and that you need to contact our Voice Authorisations team to process the transaction. The cardholder may decide not to proceed with the order. If the cardholder still wishes to proceed with the order, you will need to obtain the full card number as ePDQ only displays the first and last four digits.

2. You will need to contact either the Barclays Voice Authorisations centre on 0844 822 2000 or the American Express Authorisations number (provided to you upon successful application to American Express) and advise them that you have had a referred transaction. They will ask you for information allowing them to provide an authorisation code. The most important data is the full card number.

Note: For Amex transactions, the Transaction Detail record 'Error Message' field contains the text "CALL AMEX 8973" where 8973 in this example is the 4-digit code that you should quote when you call American Express.

3. Make a note of the authorisation code you are given.
4. Log into your ePDQ store and click **Orders** from the top four options.
5. Select **Point of Sale** from the menu on the left.
6. Select Activity of **Card Transaction**.
7. Select Transaction Type of **ForceUpdatePreAuth** (if the original transaction type was PreAuth) or **ForceUpdateAuth** (if the original transaction type was Auth).
8. Enter the original order **Transaction ID.** To obtain this, see the previous page.
9. Enter the Authorisation Code obtained in step 2.
10. Select Processing Mode of **Production**.
11. Click **Process Transaction.**
12. A **Transaction Management** page will be displayed confirming your action.

A digital receipt will be provided to your customer advising the transaction has been successfully processed. If your store is configured to receive receipts, a copy of the receipt will be sent to you.

Section	Topic	Products
B Orders	**Submitting Periodic Billing (repeat) Orders**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 103

If your web site business has customers who wish to pay by subscription, or wish to spread the cost of their order over time, you can use the Periodic Billing functionality. This allows you to enter card details once, and then allow the ePDQ engine to automatically re-submit orders. Periodic Billing is not permitted on Solo or Maestro cards.

There are two types of periodic orders. The automated approach described above, and a more manual method. This method uses the **Group ID** to link transactions, but each transaction has to be manually entered each time.

The examples in this topic all use the automated version. If you use the API, please make sure you understand how to use "internally" and "externally" managed orders, which are detailed in the main API Guide.

To submit an automatic periodic billing transaction via the **Point of Sale**:

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Select the Transaction Type of either **PreAuth** or **Auth** as required. Note that all subsequent transactions will be submitted as the same type – therefore if you submit PreAuth periodic billing transactions you will have to mark them as shipped.

Complete all mandatory fields and any optional fields you may require. The **Total** should be the amount that will be charged to the card each time and not the cumulative total. For example, if you wish to spread £100 over 4 payments, you should enter a total of £25.

5. In the **Periodic Billing Information** section, select **Periodic Order (automated transaction)**. You will then need to enter the details dependant on how you wish to submit the transaction:
   - **Recurring** will charge the card for a specified number of times, or indefinitely.
   - **Installment** will charge the card for a specified number of times until the total amount is paid. You will have to specify the number of payments.
   - The **Period** is how often you want to charge the card (i.e. once every 4 weeks).
   - The **Total # Payments** specifies how many times you want to charge the card. If you wish to charge indefinitely, enter 999.
   - Set the environment of the first transaction.
   - Select **Process Transaction**.

Section	Topic	Products
B Orders	**Cancelling & Voiding Periodic Billing Orders**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 94-95

Cancelling a Periodic Billing Order

Due to the nature of repeat billing of cardholders, you may receive requests to stop an ongoing order, or amend the payment details. In both of these cases, you must cancel the original periodic billing order. If you need to change payment details you will need to set up a new order (this will require you to obtain new card details from the cardholder).

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity**. If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to cancel click the **Order ID.**
4. The **Order Detail** page is displayed, and further down a **Periodic Billing Detail** section will be shown. Within this section, click on the Payments link (i.e. 1 of 10).
5. The **Transaction Detail** for the periodic order is displayed. Click **Cancel Order** from the **Operations** menu on the left.
6. A confirmation message will be displayed confirming the cancelled order(s).

Voiding a Periodic Billing Order

The process of voiding a periodic billing order is similar to the standard process, however, you have to remember that you may have a number of individual transactions within an order and may need to only void a specific one.

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity**. If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to cancel click the **Order ID.**
4. The **Order Detail** page is displayed, and further down a **Periodic Billing Detail** section will be shown. Within this section, click on the **Payments** link (i.e. 1 of 10).
5. The **Transaction Detail** for the periodic order is displayed. Each order will have a **Void** check box. Select the orders you wish to void from the list displayed.
6. Select **Void Transactions** from the **Operations** menu on the left.
7. A confirmation message will be displayed confirming the cancelled order(s).

Section	Topic	Products
B Orders	**Refunding & Re-Trying Periodic Billing Orders**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 94-95

Refunding a Periodic Billing Order

The ability to refund a periodic billing order will depend on the way in which they are being submitted.

If you are using the automated method, you need to ensure that if you only wish to refund part of the order that you use the Partial Refund (Credit) method as described in "Performing Transactions such as Refund & Void".

If however, you do wish to refund the whole order, or are using the manual method of submitting Periodic Billing orders, you can use the standard method of submitting a refund.

Re-Trying a Periodic Billing Order

There may be occasions where a periodic billing order is declined part way through the billing cycle. This may be because the card has been cancelled or re-issued, the funds may no longer be available or that the card issuer has changed their policy on accepting this type of order and may decline future transactions.

In the event that a transaction is declined (for example, the 5th order in a series of 10), ePDQ will send you an email advising the transaction was declined.

You can attempt to re-submit the transaction using the **RePreAuth** or **ReAuth** transaction types. (The transaction type should match the original, i.e. if the original transaction was Auth, you should use ReAuth).

1. After you have logged into the store, click **Orders** from the top four options.
2. Select **Point of Sale** from the menu on the left.
3. Check that the Activity is **Card Transaction**.
4. Select Transaction Type of **RePreAuth** or **ReAuth**. The required screens will be displayed.
5. Complete the details as required. It is important that you enter the exact original transaction ID.
6. Press **Process Transaction.**
7. You will receive confirmation of the new status of the order.

Section	Topic	Products
C Reports	**Obtaining Order & Transaction Reports**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 7 Page 111

ePDQ provides full reporting information allowing you to track activity through your store. The reports provide you with transaction information and can be used for a variety of purposes including reconciliation, risk management review, settlement checking and general management of your web business.

As with **Orders** there are a number of standard reports you can run through the Store Admin, or by using the API. (For a list of report options available through the API see the main API Guide – this is only available for ePDQ MPI users.). The main difference is that information in the **Reports** menu is predominantly read only and does not permit further action on the transaction.

The standard reports are:

- **Orders** – this provides you with an Order Search Criteria screen. Under the main Orders menu you have two set reports:
- **Recent Activity** shows all approved orders within the last 7 days.
- **Unshipped** displays all orders that have not been marked as shipped within the current calendar month.
- **Transactions** – this provides a **Transaction Search** screen and will allow to you to search for any particular transaction within an order. There is a set report of **Recent Activity** showing all approved transactions within the last 7 days.

> **TIP! As detailed in Section B (Orders), a single cardholder purchase is known as an order. Within that order, there may be multiple transactions such as the first PreAuth, the following PostAuth and then possible a Refund. Each of these transactions has a separate transaction ID that can be used in the Transaction Search. If you wanted to find a specific refund transaction without locating the complete order, you can just enter the refund transaction ID.**

- **Items**. This is only relevant to ePDQ MPI merchants who construct orders using separate items. If you made up an order with 5 separate items, you can search for each individual item. There is a set report of **Recent Activity** showing all approved transactions within the last 7 days
- **Tax**. These search options are not commonly used by UK merchants and allow searches by tax rates.
- **Settlement**. This report provides details of all previously settled transaction files. More detail is provided later in this section.
- **Batch Authorisation – This is not supported**

Section	Topic	Products
C Reports	**Using Reports for Information Purposes**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 7 Page 111

The most common use of the reporting functionality is to gauge how much business you are doing through your ePDQ store. The reports available will give full information relating to orders within any specified time period but also allow you to search based on a number of different criteria.

The search criteria for finding an order is the same used as in the main Orders tab, although when the data is displayed it is read only. You still have the ability to look further into the order by looking at the **Order Detail** or **Transaction Detail** pages.

As an example, if you wanted to know the following:

How many Visa card transactions still need to shipped from last month?

1. After you have logged into the store, click **Reports** from the top four options.
2. Select **Orders** from the menu on the left. **The Order Search** Criteria page is displayed.
3. Select **Card Type and Time** from the **Search by** drop down option. A new drop down box appears below.
4. Select the **Card type** of **Visa** from the drop down list.
5. Select the **Transaction State** of **Unshipped**.
6. Leave the defaulted selection of **Transaction Result** as **Approved**.
7. Within the **Time** options, select **Last Month** from the first drop down box.
8. Select any **Optional Fields** to be displayed in your report.
9. Press **Search**. A list of all Visa card transactions that remain as unshipped and were processed last month will be displayed in the **Order Search Results** screen.

Remember that this only provides a report of the transactions that remain unshipped. If you wish to ship the transactions, you will need to use the **Orders** main menu and find the orders. You can use the same criteria to find the orders. See "Marking a Transaction as Shipped" in Section B.

As you cannot perform any actions on orders displayed within the Reports you may wish to only provide Reports access to staff required to perform order reporting or reconciliation.

Full details of what can appear in the **Transaction Detail** fields are provided in the main Store Administrator Guide from page 127.

Section	Topic	Products
C Reports	Using Reports for Reconciliation	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 7 Page 144

When processing orders through ePDQ, you will need to reconcile to both your bank account and your monthly acquiring statement.

ePDQ allows you to check, on a daily basis what transactions have been settled and paid into your bank account. Transactions are grouped into "batches" (typically a days trading will be in a batch). You can use this report to ensure that all transactions have been processed correctly.

To run a report to show settled transactions:

1. After you have logged into the store, click Reports from the top four options.
2. Select Settlement from the menu on the left. The Settlement search screen will be displayed.
3. Select the display criteria you wish to see. Your options are:
   - **All**. Displays all settlement batches during the specified time.
   - **Approved**. Only displays approved settlement batches.
   - **Pending**. Displays settlement batches that have not completed settlement but have started the process (i.e. you may run the report during a settlement cycle).
   - **Error**. If any error occurred during settlement or the settlement batch contained incorrect data, the settlement may not complete. If you see an Error message, you should contact us. You can see the reason for the error by selecting Description within the optional display fields.
   - **Locked**. Contains settlement batches that did not complete the settlement process. These require intervention by Barclaycard Business to resubmit the settlement file. Contact us if you see this message.
   - **Cancelled**. This will only occur if we stop the settlement process.
   - **Settlements with declined transactions**. Contains settlement files where certain transactions may have been declined during settlement (i.e. they may contain incomplete data).
   - **Current Batch Detail**. This will display all transactions that are ready to be settled and will be picked up in the next settlement run.

For this example, select All, and set the optional field to show **Description**. The **Order ID** field is selected as default.

4. Enter the **Time** period you wish to search for (i.e. **Yesterday**) and click **Search**.

5. All settlement records will be displayed. Each settlement record will display the following:
   - **Settlement ID**. This is a unique ID allocated to the settlement batch and contains all transaction records settled in the batch. You should quote this to us if you ever have a query with the settlement file. The Settlement ID is a hypertext link.
   - **Status.** Confirms the status of the settlement file. See last page for a description of each status.
   - **Description (if selected in search criteria).** Provides information on the settlement file. If the status is Approved, there will not be any information here.
   - **Time.** The date and time the settlement completed.
   - **Credit Total.** The total of any refunds processed in the settlement file.
   - **Sale Total.** The total of all approved transactions in the settlement file.
   - **Total.** The net total of the settlement file.

TIP! If you submit American Express transactions, you should also select Processor Name to display which processor the settlement file was submitted to.

6. To view the contents of the settlement batch, click on the Settlement ID. This will provide you with a breakdown of transactions that have been settled and will appear on your bank account and merchant statement.

Settlement & Reconciliation Tips.

- Always use the settlement report to reconcile to your bank account as this confirms what has been paid.
- If you believe there is a discrepancy, run a settlement report that shows **ALL** settlement reports to identify if any files were unsuccessful.
- If a settlement file has been successful, but you believe a transaction is missing, run the same report within the **Reports** section. It may be that a certain transaction was actually declined, or that it was past the settlement file cut off. (See Section E, Administration for details of settlement cut offs).
- Common reconciliation mis-matches occur when transactions have been approved but have not been marked as shipped. If this is the case, they will not have been passed for settlement. Run a report that shows all **Unshipped** transactions to see if transactions are still waiting shipment.
- Other mis-matches can occur when transactions have been marked as fraudulent and are in a review status. These will require action before they will be settled. For more information on fraudulent transactions see Section D, Risk Management.

Section	Topic	Products
D Risk & Fraud	**Risk Management**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 6 Page 109 Risk Manager Guide 5.9.

As well as core transaction processing, ePDQ provides a very comprehensive Risk Management module. This provides standard rules, lists and default checks that can be used to try and identify and alert you to potentially fraudulent transactions.

Risk Management systems such as that offered by ePDQ, can help you to recognise and hopefully remove fraudulent transactions from being processed through your business.

No Risk Management system can definitively determine whether any given transaction is, in fact, fraudulent. Therefore, fraud protection systems can form only one part of a comprehensive business decision-making process that involves human oversight and investigation of each transaction in question.

The responsibility to instill such a review process lies with your general business policies on risk and not with the Barclaycard Business ePDQ product.

The information in this section provides you with instructions on how you may wish to implement strategy rules. You must ensure that you periodically review which risk management tools are effective for your business and should ensure you understand what volume of transactions are being rejected by your strategy rules.

This section details the most common risk management tools adopted and provides examples of strategy rules, lists and velocity checks that you may wish to use.

IMPORTANT! All strategy rules examples are provided in good faith to enhance your understanding of how to effectively use the Risk Management features of ePDQ. We are unable to test these strategy rules for each individual application and therefore recommend that you set the action on any new strategy rules to "Review" to ensure they meet your business requirements.

By default all Strategy rules are INACTIVE. You must choose which rules to activate.

If activated, you should then manually accept or reject the transaction. If the fraud rule is not triggered when you believe it should be, please contact us immediately. You use all strategy rules at your own risk. Barclaycard Business does not accept liability for any losses incurred as a result of any fraud rule(s) activating incorrectly, failing to activate or operating in an unanticipated manner.

Section	Topic	Products
D Risk & Fraud	**Familiarising yourself with Strategy rules**	CPI MPI Lite

Main Document Reference	Risk Manager Guide 5.9, Chapter 4 Page 31

ePDQ provides a set of standard strategy rules. When working with strategy rules, it is important that you understand how they work, and how to create new rules to suit your business.

To view the strategy rules:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The **Where are my Strategy Rules?** page is displayed.
3. Select Click here to view **My Rules.** The standard set of strategy rules are displayed.

TIP! By default, all of the strategy rules are inactive. You have to manually activate a fraud rule before it will function.

You can view the details of what the rule does by clicking on the relevant **Rule Name**. This displays the **My Rules Editor** page and shows the template screen for all new rules. The rule editor page displays the various components of the rule. These are:

- **Rule Name**. Either the standard or bespoke name assigned to a rule. If you create your own names you should ensure they are meaningful and relevant.
- **Description**. If you create your own description you should ensure it is meaningful and relevant.
- **Active**. The option to activate the rule. This must be selected for the rule to function.
- **Process Phase**. This determines whether the rule will be invoked before or after ePDQ attempts authorisation. Set to **Pre-Process** for before, or **Post-Process** for after. Some rules (such as AVS) can only be Post-Process.
- **Rule Weight.** Assign a numeric weight to the rule to control the impact a rule has on determining if a transaction is fraudulent. Further information on Weights can be found in the Risk Manager Guide "Using Rule Weighting" on page 128.
- **Rule Expression.** This shows the parameters of the rule being applied. You can write an expression directly into the expression box, or you can build an expression using the Attribute, Operator and Value fields.
- **Attribute.** This is the parameter that the fraud rule looks for to apply its checks, such as Card Number or Billing Name.
- **Operator**. Defines how you wish to treat the attribute (i.e. "equals", ""greater than", "does not equal").
-

- **Free Form Value**. Allows you to enter a specific value for the rule to look for. For example, if the Attribute you select is Billing Name, the value could be "John Smith".
- **Calculated Value**. Defines a value such as current month, in which the engine calculates which month the transaction is being evaluated in. Further information on Calculated Values can be found in the Risk Manager Guide on page 48.
- **Action.** Applies an action to rule if the transaction criteria meets the rule parameters. If the rule is triggered, the options are:
  - **Accept**. Allows the transaction to be processed.
  - **Reject**. Will stop the transaction being processed and will return a declined response to the cardholder.
  - **Review**. Holds the transaction in a pending state until you manually either accept or reject the transaction.
  - **Notify.** Lets you know via email that a transaction has triggered a fraud rule but does not interrupt transaction processing.
  - **Trace**. Lets you know via an API message that a transaction has triggered a fraud rule but does not interrupt transaction processing. This is only valid for ePDQ MPI users.
- **Action on Missing Value**. This can be applied if you wish to trigger a rule because a cardholder fails to submit a value (for example, email address). The actions associated are the same as above.
- **Rule Auto Actions.** This can be applied if you want the rule to add values to one or more block/accept lists. Further information on **Rule Auto Actions** can be found in the Risk Manager Guide, for instructions on how to create rules that add values to a list, see page 79.
- **Merchant Message**. This is displayed in the Store Admin should the transaction be identified by a fraud rule.
- **Consumer Message**. This can only be used if you use the ePDQ MPI product.
- **Send e- mail notification to.** Allows you to specify an additional email address for the merchant message to be sent. This could be sent to your admin team, or to a specific fraud team.

Each of the standard strategy rules have all of the above configured. It may be beneficial to review some of the standard strategy rules to familiarise yourself with how each parameter can be configured.

When you initially start to use strategy rules we would recommend that you only activate two or three and monitor the impact they are having on your transaction processing. It may also be prudent to adjust the **Action** on any active strategy rules to **Notify** so that you can monitor levels of transactions triggering strategy rules without impacting customers.

TIP! If you have regular customers that you do not wish to be checked by strategy rules, you can create a new rule and set the Attribute to be their card number or name, and then set the Action to "Accept". If you put this as the first rule in the sequence their transaction will not be checked by any other strategy rules.

Section	Topic	Products
D Risk & Fraud	**Adding a New Fraud Rule**	CPI MPI Lite

Main Document Reference	Risk Manager Guide 5.9, Chapter 5 Page 39

You can create new rules, specific to your business, or can create different variations of the standard rule suite. The examples below show how to create new rules to:

- Review transactions submitted with a delivery country of UK.
- Accept all transactions from cardholder John Smith from Northampton.
- Reject any transactions that have a CV2 result of "not matched".

All new strategy rules are created from the My Rules Strategy. To access this:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The **Where are my fraud rules**? page is displayed.
3. Select **Click here** to view your rules. The standard set of strategy rules are displayed.
4. Scroll down to the bottom and select **Add. A My Rules: New Rule** page will be displayed with a blank template **New Rule**.

Example 1 - Review transactions submitted with a delivery country of UK.

1. On the **New Rule** page enter the Rule Name. For this example enter "Block UK Delivery".
2. Select the **Active** flag
3. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
4. Select **Attribute of Order Form Lists** and **ShipToCountry**.
5. Select the **Operator** of **=(Equal To or In)**.
6. Select **Free Form Value** and enter the three digit country code into the **Value** field. For UK this would 826. A full list of country codes is provided in the Store Admin Guide in Appendix D.
7. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
8. Set the **Action** to **Review.** This will mean that if any transactions meet this criteria, they will be flagged as potentially fraudulent and will be placed in a review queue.
9. Set the **Action On Missing Value** to **Review** as well. This means that if the cardholder fails to enter any delivery country, the transaction will be marked for review. Please remember that this will apply to any country, not just the UK.
10. Create a Merchant and Consumer Message as appropriate.

11. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email** to field.
12. If you are happy with the details you have entered, then press Save at the bottom of the page. The rule will now be active.

With any new rule, its sequence number is set to be the last rule checked. You can change the sequence number by overwriting a new value in the Seq # field.

Example 2 - Accept all transactions from cardholder John Smith from Northampton.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name**. For this example enter "Accept John Smith".
3. Select the **Active** flag
4. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation and before any other rules are checked.
5. Select **Attribute of Order Form Lists** and **BillToName.**
6. Select the **Operator** of = **(Equal To or In)**.
7. Select **Free Form Value** and enter the **Value** of John Smith. The Value is case sensitive so would not pick up john smith.
8. Click the **Add to Rule** button. The expression you have just built will be entered into the expression box.

As you are checking two attributes (name and town), you have to enter the second attribute.

9. Click **AND (&)** to add a second attribute. This will mean that the transaction will look for details that contain John Smith AND Northampton.
10. Select the **Attribute** of **BillToCity**.
11. Select the **Operator** of = **(Equal To or In).**
12. Enter the **Value** of Northampton.
13. Click the **Add to Expression** button. The additional expression you have just built will be entered into the expression box.
14. Set the **Action** to **Accept**. You can leave the **Action On Missing Value** blank as you are looking for specific details.
15. Create a Merchant and Consumer Message as appropriate.
16. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

The rule will now be listed with the other standard rules. You should change the **Seq #** to 1, so that this rule is checked first and will allow John Smith from Northampton to go straight for authorisation without any further checks.

To change the sequence, overwrite the existing number with the new sequence number and click **in a clear space on the page**. The new order will be displayed.

Example 3 - Reject any transactions that have a CV2 result of "not checked".

The standard CV2 rule is only triggered when the response is "Not Matched". This delivers a "Cvv2Response code" of "2". If any other response is returned the rule would not be triggered.

You may wish to support your risk policy by also checking transactions where the CV2 result was anything other than "Not Matched"

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name**. For this example enter "Block CV2 Not Checked".
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process** as this rule has to check the CV2 result returned from the card issuer.
5. Select **Attribute of Order Form Fields** and **Cvv2Response.**
6. Select **Operator** of **=(Equal To or In)**.
7. Enter **Value** of **3**. For a list of possible values, see the Risk Manager Guide, page 244-245.
8. Click the **Add to Expression** button.

   TIP! You could broaden the range of not checked responses by selecting "OR" within the expression builder, and then adding further attributes, such as 5, 6 or 7. You will need to Click the Add to Expression button after you change each value. The expression would be:

   {Cvv2Response} = "3" | {Cvv2Response} = "5" | {Cvv2Response} = "6" | {Cvv2Response} = "7"

9. Set the **Action** to **Reject**. This means that any transaction that is returned with any of the CVV2 responses above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

The rule will be placed at the bottom of the standard rule sequence. Change the sequence number if you wish this rule to be activated earlier in the rule order.

Section	Topic	Products
D Risk & Fraud	**Finding Fraudulent Transactions**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 10 Page 153

Whenever a strategy rule is triggered that identifies a transaction as potentially fraudulent the details are added to a list. You can view this list to identify the level of transactions being processed through your store that trigger your strategy rules.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Under the **Transactions** menu on the left, you have two options:

   - **Fraudulent.** This will provide a search screen allowing you to search for transactions that have been marked as fraudulent. Enter your search criteria and click search to see a list of fraudulent orders.

   You can display:

   - **All** transactions which will return all transactions that have been marked for review.
   - **Review**. Those transactions that have to be reviewed and either accepted or rejected.
   - **Accepted**. Transactions that have already been reviewed and have been accepted.
   - **Rejected**. Transactions that have already been reviewed and have been rejected.
   - **Voided**. Transactions that have already been reviewed and have been void.
   - **Chargeback**. This will provide search a screen that allows you to search for all transactions that you have marked as receiving a chargeback

- **Review.** With each fraud rule, you can set the action to Accept, Reject, Review, Notify or Alert. This option will provide a list of all transactions that have been marked for review. For each transaction you will have an "Approve" or "Reject" option.

Reviewing transactions is a manual process and will require you to make a decision on whether to approve or reject the transaction. This decision may be based on additional information you have gained from the cardholder (i.e. the cardholder may have provided you with additional security information).

Section	Topic	Products
D Risk & Fraud	**Reviewing Fraudulent Transactions**	CPI MPI Lite

Main Document Reference	Risk Manager Guide 5.9, Chapter 10 Page 153

If you have the **Action** on any strategy rules set to **Review** then these transactions require further action to be completed. The transactions falling into this category can be viewed by following the instructions in the last section.

When dealing with transactions in review state you must be clear on what type of transaction they are, as the process is different for PreAuth and Auth transactions.

- **PreAuth** transactions that you approve must also be marked as shipped. Simply selecting "Approve" will not place the transaction in the settlement batch. If you do approve the transaction, you should then follow the instructions shown in "Marking a Transaction Shipped" in Section B.
- **Auth** transactions will automatically be placed in the settlement batch once you approve them.

To review a transaction:

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Under the **Transactions** menu on the left, select **Review**. A list of all transactions requiring review will be displayed. Each transaction will have an **Approve** or **Reject** check box.
3. If you wish to see which fraud rule was triggered by this transaction, click the **Order ID**. This will display the **Order Detail Page**. If you then click on the **Transaction ID** that is marked as fraud, the **Fraud Rule ID** will be displayed.
4. Once you have identified which transaction you wish to review, select either the **Approve** or **Reject** check box.
5. Click **Set Review Status** under the **Operations** menu on the left.
6. A **Transaction Management** page will be displayed confirming your action.

You must ensure that if the transaction was a **PreAuth** transaction type that you also mark it for shipment. Failure to do this will result in the transaction not being settled.

Section	Topic	Products
D Risk & Fraud	**Recording Chargebacks**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 5 Page 97

You may at some stage, be charged back for a transaction. This means that you will be required to pay back the money for the transaction to the card issuer. Whilst you can use some of the techniques offered by ePDQ to limit the number of chargebacks you receive, you may not be able to avoid them completely.

It is very important to record when a chargeback has been received. By doing this, ePDQ automatically records the card number used and adds it to a Block list. This way, if the card is presented again, it will be declined or put into a review state if you are using the strategy rules.

To record a chargeback, you first have to locate the transaction in ePDQ, an order must be settled in order for it to be recorded as a chargeback. This can be done by searching for the transaction by the card number, or by the date and time. Follow the instructions in "Finding and Order by Order ID" and instead of searching by order ID, search by card number and date.

Once you have located the transaction, you should check it is the correct order, and then follow the instructions below:

1. Click the **Order ID** of the order. The **Order Detail Page** is displayed.
2. An option of **Chargeback** is available under the Operations menu on the left. Click **Chargeback** to display the **Chargeback Management** page.
3. Select the box to the left of the transaction you want to record as a chargeback.
4. Select the reason for the chargeback (as displayed on your chargeback letter).
5. Click **Submit Chargeback** from the menu on the left. The transaction has now been marked as a chargeback. A **Transaction Management Response** page will be displayed.

TIP! You must activate the block cardnumber fraud rule to ensure that any transactions marked as chargebacks are added to the block card list and checked each time. This will ensure the same card number is not accepted again.

TIP! If you have more than one ePDQ store, you will have to manually add any cards you wish to block to each store.

Section	Topic	Products
D Risk & Fraud	**Address Verification Service (AVS)**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Appendix 8 Page 243

Address Verification is a UK based service that checks the details supplied for the cardholders billing address and post code against that held on the Card Issuers records. ePDQ simply passes the address information and receive the AVS response from the issuer. We are not responsible for the values returned.

Two components of the address are checked; the numerics of the house number and the numerics of the postcode. For example, if 1 High Street, NN4 7SG was the address, ePDQ would submit "1, 4, 7". The card issuer would then check these details and return a response based on what values match. The potential results returned are:

Response Code	AVS Display	Description
S1	(Blank)	AVS not checked (see TIP)
B1	YN	Post code not checked; address match,
B2	NN	Post code not checked; address no match
B3	NN	Post code not checked; address partial match
B4	NY	Post code match; address not checked
EX	YY	Address and Post code match
B5	NY	Post code match; address no match
B6	NY	Post code match; address partial match
B7	NN	Post code no match; address not checked
B8	YN	Post code no match; address match
N	NN	None match
B9	NN	Post code no match; address partial match
BA	NN	Post code partial match; address not checked
BB	YN	Post code partial match; address match
BC	NN	Post code partial match; address no match
BD	NN	Post code partial match; address partial match
7	UU	Response not valid (see TIP)

There are two standard AVS rules. These are only triggered for a non match:

- AVS Address Does Not Match. Triggered on NY or NN.
- AVS Zip Does Not Match. Triggered on YN or NN.

TIP! The standard rules will not be triggered for AVS not checked (Blank/S1) or Response not valid (UU/7). You may wish to set up a separate fraud rule to capture and act on these responses. See the next Topic for more information.

Section	Topic	Products
D Risk & Fraud	**Adding Additional AVS Rules**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Appendix B Page 243

The standard AVS rules are only triggered if the AVS result is returned as failed, and uses the generic "Y" and "N". This leads to very general checking as there are only four responses (YY, YN, NY and NN). You can create additional strategy rules that use the more detailed Response Codes shown on the last page to create more bespoke AVS checking and to block orders at a more detailed level.

The example below is based on a fraud rule where you only wish to reject any transactions that completely failed the post code match and only had a partial address match.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter the **Rule Name**. For this example enter "BlockAVSRule1".
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process** as this rule has to check the AVS result returned from the card issuer.
5. Select **Attribute Order Form Lists** and **AVSResponseCode**.
6. Select **Operator** of **=(Equal To or In)**.
7. Enter **Value** of **B9**.
8. Click the **Add to Expression** button. The expression will be added to the expression box.
9. Set the **Action** to **Reject**. This means that any transaction that is returned with the specific AVS Response above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered then press **Save** at the bottom of the page. The rule will now be active.

If you only wish to use your bespoke AVS rules, you should ensure that no others are activated.

As with other examples in this section, you can add multiple attributes using the **AND** or **OR** options.

Section	Topic	Products
D Risk & Fraud	**Card Security Code (CSC) (CV2)**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Appendix B Page 244 - 245

The Card Security Code is the unique 3 digit code on the rear of most cards, and 4 digit code on the front of American Express cards. It is used to identify that the cardholder has possession of the card at the time of purchase. The CSC is also referred to as CV2, Cvv2 and CVM. The table below displays the name displayed for results supplied.

The CSC data cannot be stored by you or us and must not be displayed on any receipt.

As with Address Verification, the CSC supplied is sent to the card issuer in the authorisation record. The card issuer will then check their records to confirm whether the submitted data matches. ePDQ simply passes the card security data and receives the CSC response from the issuer. We are not responsible for the values returned. The responses returned from the issuer could be:

CVM Response	CCE Response (ePDQ)	Description
2	1	CSC matches
4	2	CSC does not match issuer value
1	3	CSC was not processed
Unknown	6	CSC invalid or missing
X	7	No response from server

TIP! The default ePDQ Fraud Rule "CVV2 DoesNotMatch" will only be triggered by a CSC response of 2. No other response from an issuer will trigger the rule. You can however, set up your own rule to check for other responses.

1. Ensure that you have opened up a new blank template rule.
2. On the **New Rule** page enter a **Rule Name**.
3. Select the **Active** flag
4. Select the **Process Phase** of **Post-Process.**
5. Select **Attribute of Order Form Lists** and **Cvv2Response**.
6. Select **Operator** of **=(Equal To or In).**
7. Enter **Value** of **3. TIP! You can add further values to the expression (i.e. 6 & 7) to catch all.**
8. Click the **Add to Expression** button. The expression will be added to the expression box.
9. Set the **Action** to **Reject**. This means that any transaction that is returned with the specific CSC Response(s) above will be rejected as potential fraud.
10. Create a Merchant and Consumer Message as appropriate.
11. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

Section	Topic	Products
D Risk & Fraud	**Points to remember for using AVS and CSC checks**	CPI MPI Lite

The information provided below is to help you understand the Address Verification and Card Security Code checks.

- The company that issued the card is responsible for performing the Card Security Code and Address checks. It will also provide you with verification responses. We will not be able to give advice concerning the reason for a particular decision.

- You should make sure that Card Security Code and Address verification information is never stored on file (i.e. we recommend that you do not pre-populate this data from a cardholder database as it may have changed.). Instead, this information should be obtained from the cardholder for each transaction. The service can be used for first or individual transactions, but not for recurring transactions using the same card details.

- It is your decision whether or not to proceed with the transaction after the response has been received from the company that issued the card. These extra checks have been designed to help you decide whether or not to proceed with the transaction. The card Security Code and Address Verification Service is not an absolute guarantee of payment, but a valuable additional check.

- You must activate the ePDQ strategy rules to allow ePDQ to take any action on responses received. Whilst, ePDQ will submit Card Security Code and Address Verification information, the responses will only be returned for information and presented in the Order Detail. To either Accept, Reject or Review transactions based on the AVS or CSC responses you must have activated the strategy rules.

- You must fully understand which responses will trigger the default rules. They will not be triggered by all possible responses returned by the issuer. Please see the previous topics for further information on what will trigger the rules.

- AVS and CSC checks are applicable for all currency types.

- AVS checks are applicable for UK issued cards only.

- CSC checks are applicable for Global issued cards

- AVS and CSC are supported on Visa, MasterCard and Maestro card types only.

Section	Topic	Products
D Risk & Fraud	**Fraud Rule Responses for the ePDQ CPI**	CPI

If you are using the ePDQ CPI, you will typically receive the responses of either success or declined.

You must be aware, however, that if you activate strategy rules, additional responses will be sent from the CPI to your web site. When integrating the CPI you must cater for this and should not restrict your web site to only handle success or decline messages.

Please ensure you have configured your Post URL script to handle the additional responses sent back to your site once a fraud rule has been activated.

For more information, refer to the CPI Integration Guide or contact your web developer.

Section	Topic	Products
D Risk & Fraud	**Internet Authentication (Verified by Visa & SecureCode)**	CPI MPI

Main Document Reference	Store Administrator Guide, Appendix B Page 167

Background

ePDQ CPI and MPI users can benefit from enhanced protection against chargebacks afforded by Internet Authentication services such as Verified by Visa for Visa cards and SecureCode for MasterCard and Maestro cards. ePDQ Lite merchants cannot use these services as it requires the cardholder to enter personal information on the payment page.

Authentication services require the cardholder to authenticate themselves by the use of a secure PIN or password at the point of purchase. This is achieved by your web site displaying a specific pop up box or page containing information supplied by the card issuer to authenticate their cardholder.

To participate in the service you must have registered with us. MPI users are required to have correctly integrated their Authentication software. CPI users require no additional integration but must instruct us that they wish to use these services.

How you may benefit

As described above, by asking the cardholder to authenticate their identity the likelihood for fraud is greatly reduced. A fraudster will be unable to simply enter a card number to fraudulently obtain goods and services. Anybody attempting to use a card that does not belong to them will have to know the authentication information.

Even if the card is not enrolled in the Authentication services, you as a merchant can still benefit from 'attempted authentication'. It is important that you read and understand our Internet Authentication Procedure Guide to identify when this is possible.

Whilst Verified by Visa and SecureCode authenticates the cardholder, you must still check the card. This is done using the standard authorisation process. It is at this stage that the other risk management rules can be applied.

An example of this is where a cardholder correctly authenticates themselves but has provided an address that you will not deliver to – in this scenario despite authentication being successful, the transaction may be declined or marked for review.

IMPORTANT – Internet Authentication is an additional tool to help reduce fraud. You must also use the risk management tools provided to further reduce your risk. We advise against using Internet Authentication as your only means of fraud protection

Section	Topic	Products
D Risk & Fraud	**Authentication Results**	CPI MPI

Main Document Reference	Store Administrator Guide, Appendix B Page 167

If you have signed up for ePDQ and have activated the authentication software, you will receive an authentication response for Visa, MasterCard and Maestro transactions processed through your web site.

Depending on the liability shift available (as detailed in the Internet Authentication Procedure Guide, (which will be provided when you sign up for the service), you will be afforded protection against certain chargebacks.

The results returned by ePDQ for authentication transactions are:

Payer Security Level Value	Message	What this means.
0	Authentication is not supported.	No liability shift.
1	Authentication is supported, but the cardholder is not enrolled.	Attempted liability shift subject to scheme rules.
2	Authentication supported. Authentication succeeded.	Liability shift subject to scheme rules.
3	Authentication supported. Authentication failed.	Visa – the transaction will be declined. MasterCard and Maestro – if transaction authorised by Card Issuer no liability shift.
4	Authentication supported but authentication results unavailable.	No liability shift..
5	Authentication supported, BIN not in range.	Attempted liability shift subject to scheme rules.
6	Attempted to enroll the cardholder in a payer authentication system, but the attempt was not successful.	Attempted liability shift subject to scheme rules. For Visa, an IAV should also be returned.

Visa, MasterCard and Maestro support an Issuer Authentication Value (IAV) to determine the result of an authentication response. This will be a unique value and will be displayed in the **PayerAuthenticationCode** field.

Some transactions will also have a unique transaction ID. This is used as an additional check as to the authentication history. This is displayed in the **PayerTxnID** field.

Section	Topic	Products
D Risk & Fraud	**Viewing Authentication Results**	CPI MPI

Main Document Reference	Store Administrator Guide, Appendix B Page 167-168

When you are processing transactions for authentication, you may need to know whether or not you have liability shift protection before fulfilling an order.

This topic shows how you can view the results of authentication for a transaction.

1. After you have logged into the store, click **Orders** from the top four options.
2. If the transaction was processed within the last 7 days, select **Recent Activity**. If you are unsure when the order was processed, select **Orders** from the menu on the left and enter your search criteria (see "Finding an Order by Order ID" for more information).
3. Once you have located the order you wish to view click the **Order ID**. This will open up the **Order Detail** page. Within the Order Detail, will be a list of totals and a sub total, **Transaction Detail** and **Billing Information**.
4. Click the **Transaction ID** within the **Transaction Detail** section. The **Transaction Detail** page is displayed.
5. You need to scroll down to **Processor Details** to view the authentication results. The key results you are looking for are:
   - **Payer Authentication Code**. This can be a value up to 64 characters and is the Issuer Authentication Value. (Known as CAVV for Visa and AAV for MasterCard and Maestro).
   - **Payer Security Level**. This will be one of the values as detailed in the previous topic.

There may also be other results returned. For users of the Barclaycard Business Hosted Authentication Service, this value will typically be N/A as this check is performed by the hosted solution and not by the ePDQ payment engine.

- **Payer Authentication Result Code**. This provides details of whether the Issuer Authentication Value was generated and processed correctly. A list of codes is provided on page 167 of the Store Administrator Guide.

6. Once you have viewed the results you need, you should go back to the main orders page to find further orders.

Section	Topic	Products
D Risk & Fraud	**Setting Strategy rules for Authentication**	CPI MPI

Typically, authentication results are maintained as information for a particular order. By default there are no standard strategy rules activated to look for authentication results. This is typically because most transactions subject to fraudulent activity may be covered either by full or attempted authentication liability shift.

You may however wish to set up a strategy rule that is triggered when an authentication response is negative (either not received, or the card issuer may advise that the cardholder could not successfully authenticate themselves.

IMPORTANT! Before adding any rule based on authentication you must first ensure that you understand that you may impact a transaction that has been authorised.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules**?' page is displayed.
3. Select **Click here to view My rules.** The standard set of strategy rules is displayed.
4. Scroll down to the bottom and press **Add. A My Rules New Rules** page will be displayed with a blank template fraud rule.
5. On the **New Rule** page enter the **Rule Name.**
6. Select the **Active** flag
7. Select the **Process Phase** of **Pre-Process** and the **Action** (see point 10 below) to **Reject** if you wish to discontinue with the transaction or **Post Process** if you wish to evaluate the transaction based on the authentication and authorisation response.
8. Select **Attribute of Order Form Fields** and **PayerSecurityLevel.**
9. Select the **Operator** of **=(Equal To or In).**
10. Enter the code that you wish to trigger the rule. For a failed authentication, select 3.
11. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
12. Set the **Action** to whatever you wish to do with the transaction.
13. Leave **Action On Missing Value** as none.
14. Create a Merchant and Consumer Message as appropriate.
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email** to field.
16. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

By activating this rule, any transaction that returns a Payer Security Level result of 3 will trigger the rule.

Section	Topic	Products
D Risk & Fraud	**Velocity Checks**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 103

Velocity Checking introduces the ability to track and count transactions processed through your store and apply specific attribute checks (i.e. card number) and time/counter variables. The velocity checks should be used in conjunction with strategy rules to identify and block potentially fraudulent transactions. There are three types of velocity checks available.

- Counter-Based, Constant Velocity Checks.

  These use either fixed single, or multiple attributes such as card number or billing name and count how many times the attribute(s) are submitted. You can then use a fraud rule to specify a time period in which to monitor the velocity.

- Counter-Based, Change Detection Velocity Checks.

  This enables a single or multiple fixed attribute(s) (i.e. BillToName & IP address) to be checked against a variable attribute (i.e. card number). This will track how many different card numbers have been used against the same IP and billing name, enabling identification of randomly generated card numbers.

- Value-based Velocity Checks

  The value of a specified attribute is totaled from each matching order. Value based checks can determine the total order amount that has been placed in multiple orders using a specified Attribute of card number.

To make use of a velocity you will have to incorporate a "built-in function" from the fraud rule expression builder. The built in function for Velocity Checks is "CheckVelocity".

You then create a new fraud rule that uses the velocity and specify what criteria you want to check to activate the rule. It is important to remember that the velocity checks simply count how many times a specific attribute or variable is submitted through the engine.

TIP! The Process Code you use (pre-process or post-process) will impact when the velocity is triggered. For pre-process rules the velocity will be triggered after one further transaction is processed. If you specify a "value" of 2, this will not be triggered until after 3 attempts.

Section	Topic	Products
D Risk & Fraud	**Velocity Check Examples**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 106

This topic provides an example for each of the types of attributes. By default, ePDQ does not have any velocities pre-configured. You can set up to a maximum of 20 velocities per store.

1. After you have logged into the store, click **Risk Management** from the top four options.
2. Select **Velocities** from the **Settings** menu on the left.

   A message will be displayed stating that no velocities have been created. Click **Next** to create a new velocity. The **Risk Management Velocities** page will be displayed. The name and description can be created according to your requirements. The types are:
   - Counter-based, constant
   - Counter based, change detection
   - Value based

Example 1 – Counter-based, constant

This example uses the attribute of cardnumber. We are looking to reject any transaction where the same card number is used more than twice within 1 minute (60 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type** of **Counter-based, constant.**
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use (for example, if the attribute were AVS response, you would have to use Post-Processing).
5. You can activate the velocity rule by selecting **Yes**.

TIP! Activating a velocity will have no affect on transaction processing until you link the velocity to a fraud rule that performs an action (Accept, Reject etc).

6. Select the Attribute of cardnumber and click Add Velocity Attribute.
7. Select Save New Velocity. The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

Now that you have created a velocity you can link it to a new rule which will be triggered should the criteria you set match.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules?'** page is displayed.
2. Select **Click here to view My rules.** The standard set of strategy rules is displayed
3. Scroll down to the bottom and press **Add. A My Rules New Rules** page will be displayed with a blank template fraud rule.
4. On the **New Rule Editor** page enter the **Rule Name.**
5. Select the **Active** flag
6. Select the **Process Phase** as appropriate (for this example, it should be Pre-Process).
7. Select **Attribute of Built in Function** and **Check Velocity.**
8. Select an Operator. If you wished to trigger the rule if a cardnumber is entered more than twice in 5 minutes, you should specify > **(Greater Than).**
9. Enter a **Value.** If you wish to check for occurrences of the same card number more than twice, enter **2.** (Note: For pre-process transactions this will not be triggered until after 3 attempts).
10. Click **Add to Expression.** The expression will appear in the expression box with some blank spaces, as shown below:

    ```
    {CheckVelocity(0,"",0)} > "2"
    ```

11. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,"",0) section. Using store 44, the Velocity name of "CardCheck" and a time of 60 seconds, the expression would become:

    ```
    {CheckVelocity(44,"CardCheck",60)} > "2"
    ```

12. Set the **Action.** For this example, you would set to Reject.
13. Leave **Action On Missing Value** as none.
14. Create a Merchant and Consumer Message as appropriate.
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email** to field.
16. If you are happy with the details you have entered, then press **Save** at the bottom of the page. The rule will now be active.

Example 2 – Counter-based, change-detection

This example uses the constant attribute of card number but introduces a change detection of BillToCity. This will reject any transaction where the same card number is used but the billing city is different more than 3 times in 2 minutes (120 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type of Counter-based, change-detection**.
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use.
5. You can activate the velocity rule by selecting Yes.
6. Select the **Constant Attribute** of card number and click **Add Velocity Attribute**.
7. Select the **Change-Detection Attribute** of BillToCity and click **Add Velocity Attribute**.
8. Select **Save New Velocity**. The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules?'** page is displayed.
2. Select **Click here to view My rules.** The standard set of strategy rules is displayed
3. Scroll down to the bottom and press **Add.** A **New Rule** page will be displayed with a blank template fraud rule.
4. On the **New Rule** page enter the **Rule Name.**
5. Select the **Process Phase** as appropriate (for this example, it should be Pre-Process).
6. Within the **Attribute** field, you will need to select the **Built in Function and Check Velocity.**
7. Select an Operator. As you wish to trigger the rule if the Billing City is entered more than three times in 2 minutes, you should specify **> (Greater Than).**
8. Enter a **Value.** As you wish to check for occurrences of the same Billing City more than three times, enter 3. (Note: For pre-process transactions this will not be triggered until after 4 attempts).
9. Click **Add to Expression.** The expression will appear in the expression box with some blank spaces, as shown below:

   {CheckVelocity(0,"",0)} > "3"

10. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,””,0) section. Using store 56, the Velocity name of “BillingCheck” and a time of 120 seconds, the expression would become:

{CheckVelocity(56,"BillingCheck",120)} > "3"

11. Set the **Action.** For this example, you would set to Reject.
12. Leave **Action On Missing Value** as none.
13. Create a Merchant and Consumer Message as appropriate.
14. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email** to field.
15. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

With this velocity and rule activated, the rule will be triggered if transactions are submitted where the same card number is used but the billing city changes more than three times in 2 minutes.

Example 3 – Value-based

This example uses the constant attribute of card number but introduces a value of Transaction Total (TransTotal). This can then be used to reject a card, if it has been used to generate more than a specified transaction total (e.g. £500) in the last 5 minutes (300 seconds).

Step 1. Creating the Velocity

1. From the **Risk Management Velocities** page enter an appropriate name and description.
2. Select **Type** of **Value-based.**
3. Enter a retention time (in seconds). This is the duration that the engine will retain the attribute information. Leave the default for 1 day (86400 seconds).
4. Select a **Processing Phase** of **Pre-Processing** or **Post-Processing** depending on which attribute you are going to use.
5. You can activate the velocity rule by selecting **Yes**.
6. Select the **Constant Attribute** of card number and click **Add Velocity Attribute**.
7. Select the **Value-based Attribute** of TransTotal and click **Add Velocity Attribute**.
8. Select **Save New Velocity**. The velocity will now display in the velocity list link.

Step 2. Linking the Velocity to a Fraud Rule.

1. From within the **Risk Management** section, select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules?'** page is displayed
2. Select **Click here to view My Rules.** The standard set of strategy rules are displayed.
3. Scroll down to the bottom and press **Add. A New Rule** page will be displayed with a blank template fraud rule.
4. On the **New Rule Editor** page enter the **Rule Name**.
5. Select the **Process Phase** as appropriate.
6. Within the **Attribute** field, you will need to select the **Built in Function and Check Velocity.**
7. Select an Operator. As you wish to trigger the rule if the transaction total is greater than £500 **> (Greater Than)**.
8. Enter a **Value**. As you wish to check for transaction total greater than £500 enter **500**.
9. Click **Add to Expression**. The expression will appear in the expression box with some blank spaces, as shown below:

   {CheckVelocity(0,"",0)} > "500"

10. You need to specify the store that the check applies to, the velocity check you wish to apply, and the time (in seconds) you wish to check within the (0,"",0) section. Using store 78, the Velocity name of "TransTotal" and a time of 300 seconds, the expression would become:

    {CheckVelocity(78,"TransTotal",300)} > "500"

11. Set the **Action.** For this example, you would set to Reject.
12. Leave **Action On Missing Value** as none.
13. Create a Merchant and Commerce Message as appropriate.
14. If you wish to receive an additional email advising that this rule has been triggered, enter an email in **Send notification email** to field.
15. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press Save at the bottom of the page. The rule will now be active.

With this velocity and rule activated, the rule will be triggered if transactions are submitted where the same card number and the transaction total of one, or many transactions within 300 seconds exceeds £500.

You can apply multiple constant attributes (i.e. card number and email address) and multiple change detection attribute (i.e. billing name, IP address) to try and pinpoint potential fraud. A list of the velocity checks attributes is provided in Appendix G (page 255) of the Risk Management Guide.

Section	Topic	Products
D Risk & Fraud	**Rule Weighting**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 8 Page 128

Weights are numeric values you assign to rules. By assigning weights to rules, you can control the impact a rule has on determining if a transaction is fraudulent. For example, a rule with a weight of 500 has relatively greater significance than a rule with a weight of 50. In order for weights to have an effect on rule processing, you must create at least one rule that evaluates the *TotalScore*.

A FraudShield rule can have an assigned weight that ranges between -1000 and 1000. Positive weights are assigned to rules that indicate a transaction is possibly fraudulent, while negative weights are assigned to rules that indicate a transaction is less likely to be fraudulent. The default weight assigned to a rule when no weight has been specified is zero.

An easy and effective way to utilise weights is to create a rule that evaluates a transaction's accumulated score. If the transaction’s score exceeds a specified threshold, the rule carries out an action e.g. accept, reject or review.

Fraud rule weighting allows you to tailor the **Risk Management** tool to your own fraud policy. This is done by specifying weights to rules that you wish to use, by assigning an action of “none”. You then create a separate rule to evaluate the total score of the weighted rules and after the total weight has been calculated take action (e.g. accept, reject or review) according to the final weight total (TotalScore).

With the current strategy rules, you set the order in which you want the rules to trigger, for example, You might want the rule to check for a certain name ‘Jones’ and set the action to reject this means that it will reject all orders with the name of Jones whereas your requirement may need to be more specific in that you want to reject the order from a customer with the name of Jones who lives at a certain address or using a particular card number or email address.

Alternatively, weighting allows you to create ‘Accept’ rules for loyal repeat customers who you know are genuine and you don’t want them to be penalised by other rules that you may have set.

The addition of weights to a rule are managed from the Fraudshield Rule Management page.

To access this:

1. After you have logged into the store, click Risk Management from the top four options.
2. Select Rules from the Settings menu on the left. The 'Where are my fraud rules?' page is displayed. Select Click Here to view my rules, the standard set of strategy rules is displayed.

Example – How to create a rule with weights

Scenario

You wish to block any transactions that meet the following criteria:

	Weight
• with an email address of Jones@test.co.uk	+100
• block a customer with the billing name of Jones and/or	+50
• using card number 4111111111111111	+100

1. From the **Strategy Detail** page select the rule 'BlockEmailAddress'. The **My Rule Editor** page is displayed.
2. Assign a numerical weight e.g. 100 to the rule.
3. Set the **Action** and **Action On Missing Value** field to **None.**
4. Create a Merchant and Consumer Message as appropriate.
5. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email** to field.
6. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press Save at the bottom of the page. The rule will now be active.

You now need to add the blocked email address to the **Lists.**

7. From the **Fraudshield Risk Management** page select **Lists** from the **Settings** menu on the left. The **Risk Management Lists** page is displayed.
8. From the **'I would like to'** section select **Add New List Values** (this is the default).
9. From the **'To the following list'** field select **'BlockEmailAddress'** and select **Next.**
10. In the **List Values** field add the email address to be blocked then select **Add your value to the list.**
11. Then **Save the changes to your list.**

Repeat step 1 to 11 for rule 'BlockBillingName' and rule 'BlockCardNumber'. Remember to allocate a different numerical weight for each one depending on how high you believe it to be indicative of fraud e.g. you might deem that blocking the card number is a higher weight than blocking the billing name.

You then need to create a rule that evaluates a transaction's accumulated score. If the transaction's score exceeds a specified threshold, the rule carries out an action e.g. accept, reject or review.

All new strategy rules are created from the Fraudshield Rule Management page. To access this:

1. From the **Strategy Detail** page scroll down to the bottom and press **Add. A New Rule** page will be displayed with a blank template fraud rule.
2. On the **New Rule** page enter the **Rule Name.** For this example enter "Weight score".
3. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
4. Select the **Attribute** of **Order Form Lists and TotalScore**.
5. Select the Operator of = (Equal to or IN).
6. Enter the value of the total score you wish to check, for example 200 into the **Value** field.
7. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
8. Set the **Action to Reject.** This will mean that if the sum of the rule weighting exceeds the score you entered the transaction will be flagged as potentially fraudulent and will be rejected.
9. Set the **Action On Missing Value** to **None.**
10. Create a Merchant and Consumer Message as appropriate
11. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email** to field.
12. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

TIP! It is recommended that any weighted rules come before any rules with Accept or Reject actions otherwise weighted rules will not be processed if those rules with an action evaluate to TRUE.

Section	Topic	Products
D Risk & Fraud	**Normalisation**	CPI MPI Lite

Main Document Reference	Risk Manager Guide, Chapter 7 Page 95

Address normalisation is a technique that can be used to improve street address matching during rule processing. Normalisation enables FraudShield to compensate for alternate spellings and misspellings of the same street address. (One fraud technique, for example, involves deliberately misspelling a BillTo address or a ShipTo address in order to disguise multiple orders from the same address or delivered to the same address.)

Scenario

You wish to reject all orders received from "1 the high street, NN47SG". By adding a normalised address rule, it will check for different combinations of that address such as:

1 High Street, nn47sg
1 High St, NN47SG
1 High str# NN47SG
1 Hgh Street, NN47SG
1 Hgh Str, NN47SG

All five examples are variations of the same address. Differences in spelling, punctuation, and capitalisation, however, can outsmart many address-matching routines. As a result, addresses which contain slight irregularities often fail to match properly.

FraudShield's address normalisation algorithm is more robust. FraudShield's address normalisation capabilities allow it to ignore the variations in the list above and return a match. This is because FraudShield's address normalisation algorithm creates a sophisticated representation of each address and postal code, and uses this representation to make comparisons. In the case of the five addresses listed above, all five would match because all five break down to the same normalised representation.

Example – How to create a normalised rule

All new normalised strategy rules are created from the Fraudshield Rule Management page. To access this:

1. After you have logged into the store, click **Risk Management** from the top four options.

2. Select **Rules** from the **Settings** menu on the left. The **'Where are my fraud rules?'** page is displayed. The standard set of strategy rules are displayed.
3. From the **'Where are my fraud rules?'** page, scroll down to the bottom and select **'Click here to view My Rules'.** The standard set of strategy rules are displayed.
4. Scroll down to the bottom of the page and press **Add**. A New Rule page will be displayed with a blank template fraud rule.
5. On the **New Rule** page enter the **Rule Name**. For this example enter "Normalised Address check".
6. Select the **Process Phase** of **Pre-Process** as we wish the transaction to be checked before ePDQ obtains authorisation.
7. Select the **Attribute** of **Built in Function** and **BillToNormalizedAddress**
8. Select the **Operator** of = **(Equal to or IN)**.
9. Click the **Add to Expression** button.
10. Now select the **Attribute of Standard Lists** and **BlockBillToAddressNorm**
11. Click the **Add to Expression** button. The expression you have just built will be entered into the expression box.
12. Set the **Action.** For this example, you would set to **Reject**.
13. Set the **Action On Missing Value** to None.
14. Create a Merchant and Consumer Message as appropriate
15. If you wish to receive an additional email advising that this rule has been triggered, enter an email address in **Send notification email** to field.
16. If you are happy with the details you have entered, select **Active Rule** at the top of the page and then press **Save** at the bottom of the page. The rule will now be active.

You now need to add the blocked address to the **Lists**.

17. From the **Fraudshield Risk Management** page select **Lists** from the **Settings** menu on the left. The **'Risk Management Lists?'** page is displayed.
18. From the **'I would like to'** section select **Add New List Values** (this is the default).
19. From the **'To the following list'** field select **'BlockBillToAddressNorm'** and select **Next**.
20. In the Street field add the street address to be blocked then in the **Postal code** field add the Postal code to be blocked then **Add your value to the list**. The values will then be shown in the list value.
21. Then **Save the changes to your list**

Section	Topic	Products
E Admin	**Administration**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Chapter 4 Page 41

For each ePDQ store in operation, we will set various configuration parameters allowing you to process transactions successfully.

The following will be set for your store:

- **Store.** This provides the static details of your store. **You must not amend any details on this page without prior agreement from us.**

- **Users.** This will provide a list of current users and their role, assigned to your store. You can manage users by following the procedures detailed on page 48 of the Store Administrator Guide.

- **Access Control/Role Search.** This allows you to search which roles have been allocated to users.

- **Payment. You must not amend the Routing or Processing information without prior agreement from us.**

- **Settlement.** This defines when your store is settled. By default this will be 23:00 for Sterling stores and 18:00 for Multicurrency stores. The **Mode** will be set to **Enable Automatic Settlement.** This ensures that any transactions in the current batch are picked up each day. **We recommend that you do not change these settings.**

- **Digital Receipt Configuration.** Allows you to specify who should receive a copy of the transaction digital receipt. By default all will be selected. To change this, simply uncheck the relevant box and select Update.

- **Shipping.** Software feature not supported by ePDQ.

- **Tax.** Software feature not supported by ePDQ.

If you are unsure how to manage the administration of your store please contact the eCommerce Support team. If you are in any doubt as to the impact of the changes please do not take any action until you have spoken to us.

Section	Topic	Products
E Admin	**Time Zones**	CPI MPI Lite

Main Document Reference	None

The ePDQ payment engine, database and stores all have time zones set. As the UK and majority of Europe operate daylight savings time zones, this has been reflected in the functionality of the ePDQ engine.

There are two key time zones that you need to be aware of:

- GMT Western European Summer Time (WET)

This is the **default** time zone for all new stores. This automatically adjusts for GMT (UK winter time) and BST (UK summer time). If your store is set to GMT WET, the following will occur:

  - During the winter all times will be represented in GMT.
  - During the summer (daylight savings) all times will be represented in BST (i.e. GMT plus one hour).

- GMT Standard

This maintains a constant time zone of GMT and will not make any allowances for seasonal time zone adjustments. If you wish your store to be set to constant GMT you will need to advise us. To confirm, if your store is set to GMT, the following will occur:

  - During the winter all times will be represented in GMT.
  - During the summer (daylight savings) all times will still be represented in GMT (i.e. one hour behind BST).

Other more global time zones are available. Please contact us if you have a requirement to operate your store on a different time zone.

To view the time zone for your store:

1. Access your ePDQ store using your ePDQ Level 4 user details.
2. From within the **Administration** section, select Store from the menu on the left. The **Store Configuration** page is displayed.
3. Scroll down to see the Time Zone. This will be either **WET** for GMT WET or **GMT** for standard GMT.

To change the time zone, you should select **Update** and select a new time zone from the drop down menu. You will be required to sign off and then back in to see the change. If you are unable to change the time zone please contact us for assistance.

Section	Topic	Products
E Admin	**Unlocking Users**	CPI MPI Lite

Main Document Reference	None

ePDQ will lock out a user if they incorrectly enter user ID and password details more than three times.

The default user and role we provide to you (ePDQ Level 4) can unlock any users with permissions at either the same level or lower.

Important: If you only have one user at ePDQ Level 4 and lock this user out, you will have to contact us to unlock.

If you have set up multiple users and wish to unlock them, please follow the procedure below.

1. Establish the reason why they were locked out (do they have permission to access your store).
2. Ensure that they were entering the details correctly. Remember that both user ID and password are case and space sensitive.
3. Access your ePDQ store using your ePDQ Level 4 user details.
4. From within the **Administration** section, select **Users** from the menu on the left. The **User List** page is displayed
5. Each user currently allocated to your store will be displayed.
6. The **Account State** will display whether the user is **Active** or **Locked**. The user you need to unlock will be displayed as **Locked**.
7. Select the user you wish to unlock and click **Update**. The **Update User** page will be displayed.
8. You can unlock the user by changing the **Account State** to **Active**.
9. Select **Update**. The **User List** will be displayed again with the updated details.

The locked user will now be able to access your store as long as they enter details correctly.

Section	Topic	Products
E Admin	**Error & Response Codes**	CPI MPI Lite

Main Document Reference	Store Administrator Guide, Appendix B Page 169

ePDQ will return a response code for every transaction processed by the payment engine. These are returned in the **Processor Response Code** field and will help you determine the status of the transaction.

As there are numerous different codes returned the full list is not provided in this document. Instead we have detailed the most common codes returned. For a full list, please see the main document reference above.

The **Processor Response Code** will be displayed in the **Transaction Detail Report** for approved transactions, and in the **Error Code Report** for declined transactions.

Response Code	Response Message
1	Approved
3	Referral – Call bank for manual approval
50	Declined
500	Declined – transaction considered fraudulent by Fraud component.
501	The transaction was approved by the processor. However, it failed a post-processing fraud rule and has been voided.
502	The transaction was approved by the processor. However, it failed a post-processing fraud rule and has been marked for review.

IMPORTANT. If you use the ePDQ CPI, this may return different error codes specifically to the CPI processing. These are detailed in the CPI guides.